



LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Medvetenheten inom sjukvården vid införandet av GDPR

En kvalitativ intervjustudie om medvetandegörandet av informationssäkerhet - i ljuset av GDPR

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Ann-Kathrine Berner
Emma Herlöf

Handledare: Benjamin Weaver

Examinatorer: Anders Svensson
Björn Svensson

Medvetenheten inom sjukvården vid införandet av GDPR: En kvalitativ intervjustudie om medvetandegörandet av informationssäkerhet - i ljuset av GDPR

FÖRFATTARE: Ann-Kathrine Berner och Emma Herslöf

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

FRAMLAGD: maj, 2018

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 74

NYCKELORD: Informationssäkerhet, Informationssäkerhetsmedvetenhet, Säkerhetskultur, GDPR, Policyförändring

SAMMANFATTNING:

Den 25 maj 2018 träder EU:s nya dataskyddsförordning, GDPR, i kraft. Den påverkar alla företag i hur de hanterar persondata och personuppgifter. Detta gäller även myndigheter och hälso- och sjukvården. Inom sjukvården ses oftast patienten snarare än personen, vilket kan ställa till problem för hanteringen av personuppgifter inom sjukvården. Studien ämnar att, genom en kvalitativ intervjustudie, undersöka hur sjukvården förbereder sig och dess personal inför GDPR. Studien inleds med att titta närmare på informationssäkerhet, informationssäkerhetsmedvetenhet och säkerhetskultur. Därefter följer en genomgång av de metoder som används i studien, däribland har fyra semistrukturerade intervjuer gjorts med representanter från hälso- och sjukvården. Vi har kommit fram till att organisationer behöver implementera förändringar i organisationens säkerhetspolicy för att förbättra informationssäkerheten. Vidare ser vi att en utbredd medvetenhet kring informationssäkerhet och integritet vid personuppgifter saknas i organisationerna vi studerat. Till sist kommer vi även fram till att informationssäkerhetsmedvetenhet behöver implementeras i organisationskulturen och säkerhetskulturen, snarare än bara genom utbildning och information.

Innehåll

1	Introduktion.....	1
1.1	Problemområde.....	1
1.2	Forskningsfråga.....	2
1.3	Syfte.....	2
1.4	Avgränsningar.....	2
2	Litteraturgenomgång.....	3
2.1	Informationssäkerhet.....	3
2.1.1	Informationssäkerhetspolicy.....	3
2.2	Information Security Awareness - Att skapa Informationssäkerhetsmedvetenhet.....	5
2.2.1	Medvetenhet inom sjukvården.....	6
2.2.2	Tillvägagångssätt vid medvetandegörandet av informationssäkerhet.....	7
2.3	Informationssäkerhetskultur.....	7
2.3.1	Säkerhetskultur inom sjukvården.....	8
2.4	Kontexten – GDPR.....	9
2.4.1	GDPR inom sjukvården.....	9
2.5	Teoretiskt ramverk.....	11
3	Metod.....	14
3.1	Insamling av empiriska data.....	14
3.1.1	Metodval.....	14
3.1.2	Urval av respondenter.....	14
3.1.3	Intervjuer.....	16
3.2	Analysprocessen.....	17
3.3	Undersökningskvalité.....	18
3.3.1	Validitet och reliabilitet.....	18
3.3.2	Etik.....	18
3.3.3	Kritik.....	19
4	Empiri.....	20
4.1	Empiriskt resultat.....	20
4.1.1	GDPR.....	20
4.1.2	Informationssäkerhet.....	21
4.1.3	Informationssäkerhetsmedvetenhet.....	22
4.1.3.1	Medvetenhet.....	22
4.1.3.2	Utbildning.....	24
4.1.4	Säkerhetskultur.....	24

4.1.4.1	Värdegrund	25
5	Diskussion.....	27
5.1	Informationssäkerhet	27
5.1.1	Säkerhetsbeteende	28
5.2	Informationssäkerhetsmedvetenhet	29
5.2.1	Utbildning.....	29
5.2.2	Medvetenhet	30
5.3	Säkerhetskultur	31
5.3.1	Värdegrund	32
6	Slutsats	33
6.1	Vidare forskning	34
	Appendix 1 – Intervjuguide.....	35
	Appendix 2 – Intervju 1.....	36
	Appendix 3 – Intervju 2.....	43
	Appendix 4 – Intervju 3.....	50
	Appendix 5 – Intervju 4.....	60
	Referenser.....	67

Tabeller

Tabell 1: Teoretiskt ramverk	13
Tabell 2: Respondenter.....	15

1 Introduktion

Den 25 maj 2018 träder EU:s dataskyddsförordning, General Data Protection Regulation (GDPR) i kraft. Detta innebär att, både företag och myndigheter såsom sjukvården, behöver se över hur de behandlar personuppgifter. Syftet med förordningen är att skydda ”fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter” (Datainspektionen, 2018d) och förordningen innehåller regler om hur personuppgifter ska behandlas. Förordningen innebär att alla organisationer som har med personuppgifter att göra blir påverkade och behöver därmed se över sitt sätt att arbeta med och hur de behandlar personuppgifter.

Ett vanligt problem som organisationer har, är att se på informationssäkerhet och hantering av data utifrån ett systemperspektiv (AlHogail, 2015), där informationssäkerheten kan lösas enkelt genom säkrare system. Men när det kommer till säkerhetsincidenter som är orsakade inifrån en organisation, så visar statistiken att interna användare är skyldiga till omkring 70 procent av dessa incidenter (McIlwraith, 2016). Statistiken belyser även att orsaken till dessa incidenter beror på, till största del, att personalen har gjort fel, antingen beroende på ignorans eller okunskap. Genom förbättrad förståelse för, och förändrad attityd till informationssäkerhet hade många av dessa incidenter kunnat förhindras (McIlwraith, 2016).

I en rapport om 'Cybersecurity' från en studie genomförd bland företag i Storbritannien, med drygt 1500 deltagare och 30 djupintervjuer, uttalar sig en respondent från ett medelstort företag om utbildning i säkerhet:

The only training staff require is, 'don't open emails when you don't know who the source is, and don't open attachments.' There is training needed, but... the general user needs awareness. (Klahr, Shah, Sheriffs, Rossington, & Pestell, 2017, s. 29)

Shoniregun, Dube, och Mtenzi (2010) skriver att mänskliga faktorer är svårare att lösa än tekniska frågor när det handlar om informationssäkerhet. Människor hittar sina egna arbetssätt för att underlätta sitt dagliga arbete och därav är de säkerhetskedjans svagaste länk. Organisationers syn på säkerhet och integritet behöver innefatta en mer holistisk lösning, som tar med både tekniska och mjuka frågor i sina beräkningar (Shoniregun et al., 2010). Det betonas att säkerhet är en process, att beslutsfattare bör uppmärksammas på detta och sluta se investeringar i säkerhet som en engångsaktivitet där inget mer görs eller är något som det inte återinvesteras i förrän dålig publicitet eller nyheter om problemen kommer till deras kännedom (Shoniregun et al., 2010).

1.1 Problemområde

En så stor förändring av lagstiftningen som påverkar EU-medborgares integritet, har tidigare inte skett. Eftersom GDPR har fått så pass stor uppmärksamhet i media (Di, 2018; DN, 2018; TV4, 2018), ställs högre krav och tillit till att myndigheter tar sitt ansvar. Myndigheter behöver därför påvisa kunskap om vad de behöver göra för att kunna visa att de följer förordningen (Datainspektionen, 2018d).

Då GDPR har fokus på personuppgifter och inte patientuppgifter så blir det en omställning för sjukvården som hanterar uppgifter om patienter de behandlar. Eftersom sjukvården hanterar så pass känsliga data, såsom patientens journal, diagnostisering, och behandling av patientens sjukdom. Det är därför extremt viktigt att personalen informeras om hur denna data ska behandlas och hur deras hantering av denna känsliga data kan påverka hela organisationen om något blir fel (Katsikas, 2000).

Detta i kombination med den tidigare nämnda bristen på kunskap och medvetenhet kring informationssäkerhet, väcker frågan om hur hälso- och sjukvården medvetandegör GDPR för dess medarbetare. Vi har inte funnit någon forskning om just detta, därför är detta något vi skulle vilja undersöka vidare.

1.2 Forskningsfråga

Vår forskningsfråga är följande:

Vilka utmaningar möter en organisation och dess anställda – utifrån ett medvetenhetsperspektiv – vid en stor policyförändring som berör informationssäkerhet?

1.3 Syfte

Syftet är att undersöka hur man inom sjukvården förbereder sig och sin personal på införandet av GDPR-förordningen. Med tanke på den mängd personuppgifter som sjukvården behandlar, anser vi att sjukvården är en bransch där det är viktigt att förordningen följs. Fokus kommer att ligga på hur sjukvården medvetandegör lagstiftningen för sina anställda och vilka utmaningar som förberedelserna medför. Målet med studien är att förhoppningsvis kunna bidra med kunskap om de utmaningar som finns i samband med en större policyförändring och kunna bidra med empiriskt material för att förstå ämnen såsom medvetenhet om informationssäkerhet.

1.4 Avgränsningar

Avgränsningar görs till att undersöka hur sjukvården hanterar införandet av GDPR-förordningen. Vi har dessutom valt att avgränsa oss till att inte undersöka den tekniska delen som GDPR kan påverka.

2 Litteraturgenomgång

I detta avsnitt avser vi att gå igenom litteratur som berör informationssäkerhet, informations-säkerhetsmedvetenhet (ISA) och informationssäkerhetskultur. En kort beskrivning av GDPR och dess inverkan på hälso- och sjukvården i största allmänhet, behandlas också. Avsnittet mynnar ut i ett teoretiskt ramverk som används vidare i studiens utformning men även i analysen och diskussionen av resultatet för studien.

2.1 Informationssäkerhet

Den snabba tillväxten de senaste tre årtiondena vad gäller teknologiska förändringar, har omdefinierat organisationer. Speciellt inom hälso- och sjukvården, hur de hanterar praxis om informationssäkerhet. Enligt en undersökning som HIMSS (2017) har gjort om ”Cybersecurity” så framkommer det, utav 126 respondenter som jobbar med informationssäkerhet inom hälso- och sjukvården i USA, att 71 procent av de tillfrågade avsatte en specifik andel av organisationens budget för att hantera informationssäkerhet. En huvudpraxis i dagens organisatoriska omvärld, speciellt bland dem inom hälso- och sjukvårdssektorn är att inkludera Information Security Awareness (ISA) vilket definieras som medarbetarens generella kunskap om informationssäkerhet och kännedom om informationssäkerhets policys i dennes organisation (Bulgurcu, Cavusoglu, & Benbasat, 2010).

2.1.1 Informationssäkerhetspolicy

Att skapa en informationssäkerhetspolicy hjälper organisationer att skydda dess data från obehöriga. Men att skapa en policy kan vara svårt (Flowerday & Tuyikeze, 2016). Informationssäkerhetspolicy definieras enligt Bulgurcu et al. (2010) som redogörelse av medarbetarnas roller och ansvarsområden när det kommer till att skydda organisationens informations- och teknikresurser. Om inte särskilda steg implementeras för att skapa en heltäckande informationssäkerhetspolicy så kan policyn riskera att bli redundant, otillräcklig och sakna stöd hos anställda. Vidare gör detta att policyn inte uppfyller sin funktion (Flowerday & Tuyikeze, 2016). Flowerday och Tuyikeze (2016) menar att det finns standarder för säkerhetspolicys som ska underlätta för skapandet, hanteringen och underhållet av en säkerhetspolicy, såsom ISO/IEC27002 (2013). I Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HLSF-FS 2016:40), så ska varje vårdenhet, inom hälso- och sjukvården, ha en informationssäkerhetspolicy. De ger rekommendationer om att den ska innehålla mål kring verksamhetens arbete med informationssäkerhet för att kunna säkerställa personuppgifters ”tillgänglighet, riktighet, konfidentialitet och spårbarhet” (HLSF-FS 2016:40).

I skapandeprocessen av en säkerhetspolicy behöver organisationen ta hänsyn till interna, så väl som externa influenser. Där interna syftar till bland annat personalens hantering av information kring policyn och huruvida en situation är riskfylld. Medan externa influenser kan bero på olika lagändringar som organisationen måste följa (Flowerday & Tuyikeze, 2016). Undersökningen från HIMSS (2017) beskriver även att både internt omedvetna och medvetna hot kan uppkomma mot organisationen i samband med interna risker i informationssäkerhet.

Rapporten tar vidare upp att interna hot kan pågå under en längre tid utan att bli upptäckta, och kan i värsta fall vara mer förödande för en organisation än vid ett externt angrepp mot organisationen.

McIlwraith (2016) beskriver att Organisationen för ekonomiskt samarbete och utveckling (OECD) i sina riktlinjer för säkerheten i informationssystem och nätverk som antogs 2002 (OECD, 2002), har medvetenhet som den första av sina principer. Den första principen innebär att deltagare bör vara medvetna om säkerhetsbehovet och vad organisationen kan göra för att förbättra säkerheten. Även medvetenhet om risker och tillgängliga skyddsåtgärder ingår som en del i första steget för ökad säkerhet. Det är även viktigt att medvetenhet finns om god praxis som kan implementeras för att öka säkerheten (McIlwraith, 2016). Genom att lära ut informationssäkerhet till alla intressenter, menar Knapp, Morris Jr, Marshall, och Byrd (2009) att tankesättet kring informationssäkerhet och uppföljningsarbetet av en informationssäkerhetspolicy, kan integreras i den dagliga verksamheten.

När det kommer till risker i samband med policyförändringar i IT-system, skriver Sujan (2018) att organisationer, före och under införandet av dessa förändringar, bör dokumentera identifierade risker, implementerade åtgärder för riskreducering, samt motivering till varför kvarvarande risker anses vara godtagbara. Detta görs i en rapport som kallas säkerhetsfall. Rapporten kan granskas både internt och externt, samt ska tillhandahålla en försäkran om riskbedömningen anses vara lämplig (Sujan, 2018).

McIlwraith (2016) skriver om att information från olika standarder gällande informationssäkerhet, beskrivs tydligt att säkerhetsmedvetenhet är ett fundamentalt krav om organisationer ska överväga att uppnå bästa praxis. Givet att många näringsgrenar regleras av olika lagar och regler, rekommenderas dessutom att standarder efterlevs, där säkerhetsmedvetenhet är ett föreskrivet krav. Även Shoniregun et al. (2010) nämner att, organisationer ska vara följsamma när det gäller informationssäkerhet. Det krävs att säkerhetspolicy skapas, som säkrar exempelvis hur patienters information hanteras. Samt hur policyn säkrar patienters integritet och konfidentialitet på ett sätt som följer lagar och regler. Shoniregun et al. (2010) menar vidare, för att kunna säkerställa att detta är adekvat behöver medarbetare göras medvetna om säkerhet och integritetsskydd. Detta kan göras genom korrekta och standardiserade policys, samt rutiner för utbildning. Denna process hjälper till att lägga en bra grund för efterlevnad av både lagar och standarder. Även om en organisation har rätt att skydda sig från obehöriga avslöjanden, så har de även skyldighet att ge medarbetare träning som ger dem vägledning kring vad som är tillåtet eller ej. Men även att ange lämpligt beteende när det kommer till behandling av information (Frye, 2007).

Wiles, Gudaitis, Jabbusch, Rogers, och Lowther (2012) menar att ett medvetenhetsprogram inkorporerar bestämda genomförande, gällande informationssäkerhet, in i organisationens policys. Instruktioner och standarder blir till enkla protokoll för hur känslig information kan säkras och användas i organisationen. Knapp et al. (2009) trycker också på vikten av att hålla informationspolicyn så färsk i minnet som möjligt, och ser detta som en av de största utmaningarna med implementation av en säkerhetspolicy.

2.2 Information Security Awareness - Att skapa Informations säkerhetsmedvetenhet

I Standard of Good Practice (SOGP) beskrivs att medvetenhet om informationssäkerhet upprätthålls genom effektiva program för medvetandegörande av informationssäkerhet. Där all personal som har tillgång till information samt olika informationssystem, inkluderas i programmen (McIlwraith, 2016). Medarbetare bör ges vägledning för att förstå informationssäkerhet, varför policys och standarder är viktiga att följa, samt bli medvetna om deras personliga ansvar (McIlwraith, 2016). Formella medvetenhetsprogram bör vara koordinerade individuellt eller anordnas i grupp. Programmen eller utbildningen bör ske strukturerat och specialiserat material kring informationssäkerhet, som är godkänt av ledningen. Dessa utbildningar bör vara uppdaterade med aktuell praxis och appliceras på alla individer med tillgång till information samt informationssystem. Medvetenhetsnivån bör även mätas och granskas med jämna mellanrum (McIlwraith, 2016).

McIlwraith (2016) tar vidare upp att SOGP beskriver att utbildning eller träning för medarbetare som kontrollerar eller har tillgång till information och informationssystem, bör utrustas med kunskap för att kunna bedöma säkerhetskraven, föreslå säkerhetskontroller samt säkerställa att dessa fungerar effektivt. Syftet med utbildningen bör vara att se till att systemen används korrekt och säkerhetskontrollerna används av användarna i organisationen (McIlwraith, 2016). Enligt den mest använda informationssäkerhetsstandarden BS 7799 bör alla inom organisationen samt leverantörer och tredjeparts användare, få både lämplig medvetenhetsträning och regelbundna uppdateringar gällande policys och förfaranden som är relevanta för deras arbetsuppgifter. Det förespråkas även att det bör ske löpande och vara anpassade till berördas roller och ansvarsområden (McIlwraith, 2016).

Om medarbetarna inte utbildas eller får genomgå träning, bör det inte komma som en överraskning att de kan begå misstag. Därför är det viktigt att ge medarbetarna bra träning. Låta dem veta vad de ska göra och vad de förväntas att göra. Detta då många vet inte vad deras ansvar egentligen är (McIlwraith, 2016). Bra träning minskar felen och ökar säkerheten tack vare att antalet fel minskar (McIlwraith, 2016). Wiles et al. (2012) menar även på att det inte ska antas att nyanställda är medvetna om hur känslig information ska skyddas på korrekt sätt, och ett hot kan bland annat vara oavsiktliga olyckor på grund av kunskapsbrist hos personalen. Frye (2007) menar då på att det är viktigt att ge en grund att stå på som nyanställd, så att de kan utföra sina arbetsuppgifter. Program i informationssäkerhetsmedvetenhet är till hjälp för att alla medarbetare, både nya och gamla, att förstå och uppvisa korrekt beteende när det gäller att skydda känslig information inom organisationen (Wiles et al., 2012).

Informationssäkerhetsmedvetenhet är en grundläggande del i effektiv säkerhetshantering. Dock är det inget universalmedel, det kräver både kompetens och att ett antal parallella aktiviteter uppmärksammas, till exempel uppföljning av standarder och policys, samt hjälpa medarbetarna och säkerställa att de har rätt kompetens för att utföra sitt dagliga arbete (McIlwraith, 2016). Enligt McIlwraith (2016) begår människor misstag, men det viktiga är att uppmärksamma det istället för att blunda för det. När misstagen uppmärksammas är det lättare för organisationen att undvika att dessa sker igen, och därmed minska effekten av oönskade intrång (McIlwraith, 2016).

Ghazvini och Shukur (2017) redovisar att träningsprogram kan identifiera och lägga fokus på de delar som är viktiga för organisationen och dess uppdrag. Effektiva program är mer än en årlig engångshändelse. Programmet bör inkludera kontinuerlig påverkan över hela året, samt

att innehållet levereras till medarbetarna på ett engagerat och lockade sätt för att uppmuntra till förändring av beteendet kring informationssäkerhet i det dagliga arbetet. Genom programmet förstår medarbetarna och blir följsamma inför organisationens säkerhetspolicys. Medarbetarna kan därmed aktivt känna igen, förebygga och rapportera säkerhetsincidenter (Ghazvini & Shukur, 2017).

Frye (2007) skriver att absolut säkerhet inte kan garanteras eftersom det skulle försvåra medarbetarnas dagliga arbete. Detta på grund av att det skulle ta tid att verifiera allt som krävs för att komma så nära 100 procent säkerhet som möjligt. Dock menar han att genom stark träningsregim och process för hantering av förändringar, kan organisationen sätta sig själv och sina medarbetare i bästa möjliga position när det gäller att skydda organisationens information.

2.2.1 Medvetenhet inom sjukvården

Då sjukvården jobbar med ytterst känslig information, såsom personuppgifter som kan identifiera personer genom information om sjukdomar, vanor eller behandlingar, är det därför av största vikt att ha tillräcklig medvetenhet, utbildning eller träning inom hälso- och sjukvårdsförvaltningen (Katsikas, 2000). Även Mehraeen, Ayatollahi, och Ahmadi (2016) beskriver att alla medarbetare på ett sjukhus, speciellt nyanställda behöver utbildas i vad deras ansvar är när det gäller att skydda patientinformation.

Katsikas (2000) redogör att redan för en lägsta nivå inom organisationen, bör det eftertryckligen vara att medvetenhet inte är någon form av informell eller informativ träning. Anledningen till detta är att medvetenhetsaktivitetens huvudsakliga syfte är att uppmärksamma berörda individer på säkerhet och tillåta dem att upptäcka informationssystemens säkerhetsbetydelse. Samt hur de ska reagera i enlighet med det. Då moderna sjukvårdsenheter har en mer teknisk miljö, så är det i princip omöjligt för någon medarbetare att utföra sina arbetsuppgifter, utan att vara medveten om säkerheten. Den naturliga slutsatsen är därför att alla medarbetare behöver medvetenhet (Katsikas, 2000).

Nästa steg är en lärandeprocess, där syftet är att ge de med speciella funktioner inom organisationen, en relevant och nödvändig säkerhetskompetens, detta kan göras genom kunskapsbyggande (Katsikas, 2000). I en studie från sjukvården i Kina fann de att medarbetare inom hälso- och sjukvården var medvetna om vikten av att lära sig av säkerhetsincidenter, medarbetarna föreslog även att exempel på säkerhetsincidenter borde inkluderas i organisationens utbildning och träning i säkerhet (He & Johnson, 2017). Träning är enligt Katsikas (2000) nödvändig för medarbetare, vars roll kräver speciell kunskap om säkerhetshot, sårbarhet, policys, hantering och kontroll. Träning är mer formell än medvetandegörande och kräver en mer aktiv roll från deltagarna, detta tar oftast längre tid. Katsikas (2000) hänvisar även till att alla medarbetare inte behöver få samma sorts träning utan vad de behöver beror på vad deras funktioner inom organisationen kräver för kunskapsnivå.

Vidare tar undersökningen från HIMSS (2017) upp att medvetenhetsprogram och utbildningar inom informationssäkerhet sker årligen för 87 procent av de tillfrågade i deras undersökning. Värt att nämna är att medvetenhetsträning och utbildning är något som krävs enligt HIPAA Security Rule som kan vara en av anledningarna till att siffran kring utbildning och medvetenhet är så pass hög. Däremot beskriver en rapport från Myndigheten för samhällsskydd och be-

redskap (MSB) från 2015 att andelen LSF-medlemmar (Läkarsekreterares och Sjukvårdsadministratörers Förbund) och sjuksköterskor som gått en lärarledd kurs i informationssäkerhet är 32 procent respektive 15 procent av de tillfrågade. Där 753 LSF-medlemmar och drygt 2700 sjuksköterskor deltog i undersökningen. Rapporten pekar på att ledningsansvar och lärarledda kurser i informationssäkerhet, har ett starkare samband med kännedom och erfarenhet av kontrollarbete. Rapporten visar även på ett ”genomgående mönstret är att kännedom och erfarenhet av kontrollarbete och incidenter samspelar med ledningsansvar och kompetens”. Där kontrollarbete exempelvis kan vara kvalitetsgranskning, logguppföljning och obehörig åtkomst (MSB, 2015).

2.2.2 Tillvägagångssätt vid medvetandegörandet av informationssäkerhet

Frye (2007) skriver om olika steg i samband med stora förändringar. Första steget är upptäckt som behandlar saker som att först beskriva anledningen till förändringarna som sker, nästa del är att vara empatisk och sista delen är att ledningen bör använda sig av tydlig kommunikation med medarbetarna. Andra steget är själva övergången i förändringar där organisationen bör vara säkra på att de förklarar fördelarna med förändringen, ledningen bör identifiera en förespråkare som kan vara ett ansikte utåt i initiativet. Vidare skrivs det att de som organiserar initiativet, bör ta till sig deltagarnas input, ha medvetenhet om initiativets timing samt organisationen bör försäkra medarbetarna om deras anställningsskydd. De två sista delarna i det andra steget är att medarbetare med ökade säkerhetsförväntningar, bör vara medvetna om att de kommer få utbildning/träning som möjliggör för dem att klara av de nya kraven samt att förändringen ska ske i en hanterbar takt (Frye, 2007). Det tredje och sista steget är åter-frysning som är delat i tre delar där första delen innebär att indikera till ledningens stöd att processen är klar och att handlingar börjar överensstämma med de nya fastställda policyerna. Andra delen innefattar att organisationen ska offentliggöra framgångar och vidta förändringar vid behov under förändringens gång, tredje delen i detta sista steg innebär att organisationen bör bistå med medarbetar tjänster (Frye, 2007).

I ett annat medvetenhetsprogram kan en del vara att påverka organisationskulturen och implementera ett säkerhetstänk i de dagliga rutinerna (Wiles et al., 2012). De föreslår ett program där samma meddelande upprepas sju gånger vid sju olika tillfällen och på sju olika sätt. Förhoppningen med själva programmet är att informationssäkerhet ska implementeras i organisationskulturens värderingar. För att en organisation ska kunna fullfölja ett sådant långsiktigt medvetenhetsprogram krävs ett gott ledarskap, samt ha processer och ha resurser på plats (Ghazvini & Shukur, 2017). Enligt Ghazvini och Shukur (2017) så tar ett sådant program cirka tre till fem år, för att kunna se någon effekt på organisationskulturen.

2.3 Informationssäkerhetskultur

Informationssäkerhetskultur: En samlad uppfattning, attityder, värderingar, antaganden och kunskap som guidar människor i interaktion med informationsmässiga tillgångar i en organisation med målet att influera anställdas säkerhetsrelaterade beteenden för att bibehålla informationssäkerheten. Fri översättning, (AlHogail & Mirza, 2014, s. 2).

McIlwraith (2016) beskriver att medvetenhet kring informationssäkerhet är ett pågående problem som organisationer måste hantera. Framst när det kommer till problem med passivitet

hos anställda som upplever att de redan kan ”allt” om exempelvis informationssäkerheten och därför inte lyssnar. Ett annat problem kan vara nya system och teknologier, där problem kan uppstå kring informationssäkerhet. Samt problem med alldeles för kortsiktiga prioriteringar och mål. McIlwraith (2016) menar vidare på att problemen kan undvikas eller minska genom att ta in ”Employee behaviour” som genom arbete med informationssäkerhet kan förbättra organisationskulturen och minska risken för dataintrång.

Den snabba utvecklingen av ny teknologi gör att organisationer utsätts för fler risker sett till informationssäkerheten. Många organisationer väljer att implementera nya kreativa metoder för att stärka informationssäkerheten i systemen för att kunna hänga med i utvecklingen och kunna stå emot dataintrång på ett bättre sätt än tidigare (AlHogail, 2015). Allt som oftast handlar det om systemen, och att informationssäkerheten förstärks rent systemmässigt, men många organisationer glömmer bort att säkerhet inte bara handlar om tekniska problem utan är även ett ’People issue’ (AlHogail, 2015).

AlHogail (2015) menar vidare att det är viktigt för en organisation att ha en organisationskultur som stödjer ett säkerhetsrelaterat tänk. Då kan organisationen lättare påverka anställda till att jobba med ett säkerhetstänk i de dagliga rutinerna samt öka personalens generella kunskap gällande informationssäkerhet. Genom att skapa värderingar som överensstämmer med ett informationssäkert tänk, kan risken för dataintrång minimeras ytterligare menar AlHogail (2015). Organisationer kan bli effektiva i dess informationssäkerhet först när de anställda förstår och accepterar nödvändiga försiktighetsåtgärder (AlHogail, 2015).

Malcolmson (2009) menar att en säkerhetskultur ”Security culture could potentially impact on the security of that organization” (Malcolmson, 2009, s. 1). Med detta menas, att de beteenden man vill åstadkomma med en säkerhetskultur, kommer utav identifiering av säkerhetsrelaterade idéer och värderingar och dessa kan i sin tur påverka anställdas beteenden (AlHogail, 2015; Ramachandran, Rao, & Goles, 2008). Säkerhetskulturen definierar därmed vilka beteenden som är acceptabla ur ett säkerhetsperspektiv och hjälper anställda i hur de ska agera i den dagliga verksamheten. Vidare menar Alfawaz, Nelson och Mohannak (2010) att införandet ett gediget ramverk krävs för att skapa en säkerhetskultur. Ramverket bör innehålla identifiering av hur kunskap, färdigheter och individuella inställningar till hur arbete ska utföras för att kunna påverka individen eller gruppen till att arbeta på ett informationssäkert sätt. De menar dessutom på att skapandet av en miljö där det ligger på allas ansvar att se till att utföra arbetsuppgifterna på rätt sätt ur ett säkerhetsperspektiv, de menar också att det leder till att ”göra rätt” blir en norm inom organisationen (Alfawaz et al., 2010).

2.3.1 Säkerhetskultur inom sjukvården

Hassan och Ismail (2016) nämner att utifrån användare av informationssystem inom sjukvården, så belyses medvetenhet som något som måste ligga inbäddat hos medarbetarna på ett kreativt sätt. Vidare beskrivs det att organisationens medarbetares attityd samt beteende har en viktig roll när det kommer till informationssäkerheten i sig, men även beteendet jämt mot andra medarbetare. I deras studie bekräftar de även att säkerhetsmedvetenhet och säkerhetsbeteende, är de viktigaste aspekterna för att belysa när det kommer till sjukvårdspersonalens informationssäkerhetskultur (Hassan & Ismail, 2016). Liknande beskriver Metalidou et al. (2014) att alla organisationer har ett behov av att förespråka en kultur där medarbetare är medvetna om hur de bör bete sig ansvarsfullt samt förstår hur det är bäst att agera när de möter potentiella säkerhets händelser.

Hassan, Maarop, Ismail och Abidin (2017) fann i sin studie om informationssäkerhetskultur inom hälso- och sjukvården, att de tre viktigaste faktorerna som betonar informationssäkerhetskulturen, är säkerhetsmedvetenhet, säkerhetskunskap och säkerhetsbeteende. Dessa faktorer behöver även stöd från ledningen för att försäkra sig om att säkerhetskultur skapas bland vårdpersonal. Vidare beskriver Hayden (2017) att inom många hälso- och sjukvårdsorganisationer är säkerhetsutbildning och medvetenhetsprogram underfinansierade. Ett resultat blir att medarbetarna inte har rätt kunskap för att se potentiella hot eller möjlighet att hitta balansen mellan säkerhet och att utföra sitt dagliga arbete. Vidare beskrivs det att en lösning är att lägga fokus på att skapa en säkerhetskultur på samma sätt som de uppmuntrar till patientsäkerhet och kvalitativ vård (Hayden, 2017).

Hayden (2017) menar att en effektiv säkerhetskultur skapas först när medarbetarna förstår vikten av att skydda information som behandlas inom organisationen. Regelbundna möten bör hållas, inte bara för att utbilda medarbetarna om säkerhetens vikt, utan även för att försäkra sig om att säkerheten inte försvårar processer i det dagliga arbetet. I slutändan kan säkerhet bli ett enhetligt organisationsmål och inte en extra uppgift eller något som skulle vara bra att ha (Hayden, 2017).

2.4 Kontexten – GDPR

Personuppgifter klassas som uppgifter som direkt eller indirekt kan identifiera en fysisk person (Datainspektionen, 2018a). Behandling av personuppgifter innefattar insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring (Datainspektionen, 2018d).

Vissa personuppgifter klassas som känsliga och har därför strängare krav, dessa avser; ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning (Datainspektionen, 2018b). Dessa uppgifter får samlas in vid särskilda tillfällen, ett av dessa tillfällen är om de samlas in och används av hälso- och sjukvård vid förebyggande hälso- och sjukvård och yrkesmedicin, fastställning av diagnoser eller vid behandlingar. Förordningen gäller när personuppgifter samlas in, bearbetas, lagras, sprids, ändras eller raderas (Datainspektionen, 2018b; Ledendal, 2018).

2.4.1 GDPR inom sjukvården

Dataskyddsförordningen påverkar sjukvården på lite andra sätt än för övriga företag. Förordningen blir i vissa avseende underordnad exempelvis patientdatalagen (Sveriges Kommuner och Landsting, 2018). Sveriges Kommuner och Landsting (2018) har skrivit i en rapport: Förändringar för hälso- och sjukvården genom EU: s dataskyddsförordningen, att de största förändringarna när det kommer till hur GDPR påverkar sjukvården är bland annat pseudonymisering. Det innebär att personuppgifter inte längre kan tillskrivas en identifierad eller identifierbar fysisk person, utan dessa uppgifter måste förvaras separat och kompletteras med vid behovet av informationen (Datainspektionen, 2018b; Sveriges Kommuner och Landsting, 2018).

Genom den nya förordningen så ska den registeransvarige inte bara följa principerna, denne ska även visa att regelverket följs på ett korrekt och ansvarsfullt sätt (Sveriges Kommuner och Landsting, 2018). Det kräver att den registreringsansvariga aktivt måste se till att förordningen efterlevs. Enligt artikel 5 är de viktigaste principerna, vad det gäller personuppgifter, laglighet, korrekthet och öppenhet, ändamålsbegränsningar, uppgiftsminimering, lagringsminimering integritet och konfidentialitet samt ansvarsskyldighet (Datainspektionen, 2018d; Sveriges Kommuner och Landsting, 2018).

En annan skillnad från tidigare lagar är att myndigheter, bland annat sjukhus och andra vårdenheter, måste kunna påvisa en laglig grund för behandlingen av personuppgifter. Detta skiljer sig i det avseendet att myndigheter inte längre kan hänvisa till intresseavvägning som man tidigare har kunnat göra (Sveriges Kommuner och Landsting, 2018). Lagliga grunder som gäller såväl för myndigheter, som för övriga företag, är bland andra; medgivande från den registrerade, att personuppgifterna är nödvändiga för att fullfölja ett ingått avtal med den registrerade, personuppgifterna är nödvändiga för att fullfölja av en rättslig förpliktelse, vitala intressen (på liv och död) samt att behandlingen av personuppgifter är nödvändig vid allmänt intresse eller myndighetsutövning (Sveriges Kommuner och Landsting, 2018).

Det ställs även krav på att redan insamlade uppgifter ska vara kompatibla med nämnda principer (Sveriges Kommuner och Landsting, 2018). Då sjukvården kan komma att behandla uppgifter som är förbjudna i artikel 9 (Datainspektionen, 2018b) och som även nämns ovan, så har sjukvården undantag från förordningen. Utöver det tidigare nämnda lagliga grunderna så är exempelvis ”arkivering av allmänintresse, vetenskaplig och historisk forskning, statistiska ändamål (med förbehåll för artikel 89 och nationell eller EU-lag)” (Sveriges Kommuner och Landsting, 2018, s. 5) och ”förebyggande yrkesmedicin, medicinska diagnoser, tillhandahållande av vård och omsorg eller behandling eller administration av hälso- eller omsorg och systemen som bygger på nationell lagstiftning eller EU-lagstiftning” (Sveriges Kommuner och Landsting, 2018, s. 5) är även giltiga undantag från förordningen.

När det kommer till den registrerades rättigheter så har förordningen skärpts och medför att sjukvården måste vara transparent, begriplig och lättillgänglig (Datainspektionen, 2018c; Sveriges Kommuner och Landsting, 2018). När det kommer till rätten att bli bortglömd, så gäller detta inte för patientjournaler, i folkhälsoändamål eller för forskningsändamål (Sveriges Kommuner och Landsting, 2018). När det gäller rätten till portabilitet så ska detta även gälla för sjukvården (Datainspektionen, 2018b).

Vidare beskriver rapporten från Sveriges Kommuner och Landsting (2018) att det finns tre ytterligare viktiga definitioner i dataskyddsförordningen som är relaterade till hälsoinformation. Den första är uppgifter om hälsa som innebär de personuppgifter som är kopplade till den registrerades fysiska eller psykiska hälsa och ger information om den registrerades hälsostatus. Den andra handlar om genetiska uppgifter, där nedärvda eller förvärvade genetiska kännetecken som kan ge information om en fysisk persons fysiologi eller ett biologiskt prov. Den sista är biometriska uppgifter, som är personuppgifter som införskaffats via teknisk behandling. Dessa kan vara antingen fysiologiska eller beteendemässiga kännetecken som kan bekräfta en persons identitet, exempelvis ansiktsbilder eller fingeravtrycksuppgifter (Datainspektionen, 2018a).

2.5 Teoretiskt ramverk

Nedan följer ett teoretiskt ramverk baserat på den genomgångna litteraturen. Ramverket ligger till grund för hur intervjuguiden är utformad, samt till diskussionsavsnittet.

Teman	Faktorer	Referenser	Frågor från intervjuguiden (se Appendix 1)
Informations-säkerhet	Informationssäkerhetspolicy och policyförändringar	Bulgurcu, Cavusoglu och Benbasat (2010) Flowerday och Tuyikeze (2016) Frye (2007) HIMSS (2017) Knapp, Morris Jr, Marshall, och Byrd (2009) McIlwraith (2016) Shoniregun, Dube, och Mtenzi (2010) Sujan (2018) Wiles, Gudaitis, Jabbusch, Rogers och Lowther (2012)	<ul style="list-style-type: none"> • Vad krävs i en organisation för att GDPR ska följas? • Har det skett en sådan här större förändring förut? • Vilka utmaningar finns inom organisationen inom GDPR?
Informations-säkerhetsmedvetenhet	Medvetenhet	Frye (2007) Ghazvini och Shukur (2017) He och Johnson (2017) HIMSS (2017) Katsikas (2000) McIlwraith (2016) Mehraeen, Ayatollahi och Ahmadi (2016) MSB (2015) Wiles, Gudaitis, Jabbusch, Rogers och Lowther (2012)	<ul style="list-style-type: none"> • Hur går man tillväga för att informera om GDPR? • Finns det en standard för medvetandegörande av stora policyförändringar såsom GDPR? • Har du varit involverad i något annat program som har haft medvetandegörande av informationssäkerhet?

	Utbildning	<p>Frye (2007)</p> <p>Ghazvini och Shukur (2017)</p> <p>He och Johnson (2017)</p> <p>Katsikas (2000)</p> <p>McIlwraith (2016)</p> <p>Mehraeen, Ayatollahi och Ahmadi (2016)</p> <p>MSB (2015)</p> <p>Wiles, Gudaitis, Jabbusch, Rogers, och Lowther (2012)</p>	<ul style="list-style-type: none"> • Hur går man tillväga för att informera om GDPR?
Säkerhetskultur	Säkerhetskultur	<p>Alfawaz, Nelson, och Mohannak (2010)</p> <p>AlHogail (2015)</p> <p>AlHogail och Mirza (2014)</p> <p>Hassan och Ismail (2016)</p> <p>Hassan, Maarop, Ismail och Abidin (2017)</p> <p>Hayden (2017)</p> <p>Malcolmson (2009)</p> <p>McIlwraith (2016)</p> <p>Metalidou et al. (2014)</p> <p>Ramachandran, Rao och Goles (2008)</p>	<ul style="list-style-type: none"> • Anser ni/du att det är viktigt att medvetandegöra GDPR för personal? • Jobbas det med informationssäkerhets medvetenhet i det dagliga arbetet?
	Värdegrund	<p>Alfawaz, Nelson, och Mohannak (2010)</p> <p>AlHogail (2015)</p> <p>AlHogail och Mirza (2014)</p> <p>Hassan och Ismail (2016)</p> <p>Hassan, Maarop, Ismail och Abidin (2017)</p> <p>Hayden (2017)</p> <p>Metalidou et al. (2014)</p> <p>McIlwraith (2016)</p> <p>Ramachandran, Rao och Goles (2008)</p>	<ul style="list-style-type: none"> • Vad tänker sig organisation att de vill uppnå med att medvetandegöra? • Har ni fått någon respons från personal på eventuella förändringar i den dagliga verksamheten eller överlag? • Jobbas det med informationssäkerhets medvetenhet i det dagliga arbetet? • Vilka utmaningar finns inom organisationen inom GDPR?
GDPR	Lagändringar	<p>Datainspektionen (2018d)</p> <p>Sveriges Kommuner och Landsting (2018)</p>	<ul style="list-style-type: none"> • Hur har förberedelserna inför GDPR sett ut?

			<ul style="list-style-type: none">• Hur har GDPR påverkat dig och dina arbetsuppgifter?• Har det skett en sådan här större förändring förut?• Har ni fått någon respons från personal på eventuella förändringar i den dagliga verksamheten eller överlag?
--	--	--	--

Tabell 1: Teoretiskt ramverk

3 Metod

Detta avsnitt innehåller beskrivning av hur vi har gått tillväga för att utföra denna studien. I detta avsnitt hålls även en diskussion om varför vissa metodval gjordes samt även en del om det kritiska förhållningssättet till studien.

3.1 Insamling av empiriska data

3.1.1 Metodval

Denna studie är baserad på kvalitativ intervjustudie där, enligt Bryman och Bell (2017), tonvikten ofta ligger på ord istället för siffror. Detta för att kunna lägga större vikt vid djupare analyser och tolkningar av den sociala verkligheten och hur deltagarna i studien tolkar sitt sammanhang (Bryman & Bell, 2017). I studien har vi därför valt att fokusera på hur respondenten tolkar och uppfattar sin verklighet, utifrån ett informationssäkerhetsperspektiv, kopplat till GDPR som ett fall. Målet är att få en djupare och nyanserad uppfattning om hur verksamheter fungerar och hur anpassningen sker till GDPR. För att sätta det i relation till hur teorier föreslår att något ska utföras. Bryman och Bell (2017) menar också på att kvalitativa studier ofta har en växelverkan mellan teori och den insamlade empirin, där analys av det empiriska materialet kan styra vilken teori som används och tvärtom. Efter varje utförd intervju med deltagarna har en revidering av exempelvis intervjuguiden och teori genomförts för att säkerställa att frågeställningen kunde besvaras på bästa sätt.

Litteraturgenomgången var baserad på artiklar och journaler inom informatik, informationssäkerhet, informationssäkerhetsmedvetenhet samt säkerhetskultur. Sökningen av litteraturen skedde via Google Scholar, LUBsearch och viss statistik är funnen via sökningar på rapporter och statistik via Googles sökmotor, dock med ett kritiskt förhållningssätt till källorna. Via LUBsearch gjordes avgränsningar att söka på ämnena i särskilda journaler, såsom större informatik journaler samt journaler som behandlar informatik inom hälso- och sjukvården.

3.1.2 Urval av respondenter

Urvalsprocessen har utgått dels från den valda frågeställningen samt även begränsningen till att titta på hur sjukvården arbetar med GDPR och medvetandegörande av lagstiftningen bland personalen. Det har resulterat i att urvalet dels har gjorts via kontaktpersoner som har kunnat rekommendera personer som på något vis jobbat, jobbar eller är införstådda med GDPR. För att få en så bred förståelse som möjligt, så har olika intervjupersoner på olika nivåer i hierarkin inom sjukvården intervjuats.

Dels har snöbollseffekten använts som en urvalsmetod, det vill säga att en kontaktperson rekommenderat någon annan och så vidare (Jacobsen, 2002). Bekvämlighetsurval har även använts (Bryman & Bell, 2017), där kontakt bland annat har skapats genom någon vi kände sedan innan. Detta för att dels kunna säkerställa att respondenter med rätt kompetens deltog i studien, men även för att dessa respondenter hade tid och möjlighet att ställa upp på en intervju. Även en spridning inom privat och offentlig vård har tagits i beaktning. Dessa kriterierna

har legat till grund för att få en så omfattande förståelse för hur GDPR påverkat sjukvården utifrån ett informationssäkerhetsperspektiv.

Respondenterna vi har intervjuat har alla varit, eller är delaktiga och införstådda med vad GDPR innebär, och vet utifrån sin position hur den nya lagstiftningen påverkar deras organisation. En initial kontakt med respondenterna har skett vi mejl där en förfrågan skickats ut till respondenterna om ett deltagande i studien (Jacobsen, 2002). Intervjuguiden skickades till alla respondenter en dag innan intervjun. Detta för att respondenten ska kunna vara mer förberedd på vilka frågor som denne skulle besvara och därmed kunna ge ett mer utförligt svar (Jacobsen, 2002). Vi ansåg inte att utskicket av intervjuguide hade någon negativ inverkan på vår studie, då frågorna vi ställde var med av en faktabaserad karaktär. Vi var därmed inte intresserade av respondenternas egna individuella upplevelser av förberedelserna inför GDPR.

De organisationer som respondenterna kom ifrån är SUS, Skånes Universitetssjukvård som ingår i Region Skåne, Unilabs har verksamhet inom öppen och sluten vård med laboriermedicin och bild- och funktionsdiagnostik, Vuxenpsykiatri i Malmö och Trelleborg som ingår i Region Skåne, samt Beroendecentrum i Malmö och Trelleborg, som även ingår i Region Skåne. Följande Tabell 2 visar vilka det är som deltagit i studien och vilken position de innehar.

Intervju	Namn	Organisation	Roll	Plats	Intervjutyp / längd	Appendix
1	Olivia Hjorth	SUS	Kanslichef, projektledare för inventering av GDPR	Lund	Personligt möte / 43 min	2
2	Karim Ben Fredj	Unilabs, Radio- logi Sverige	Verksamhets- utvecklare	Lund	Skypemöte / 36 min	3
3	Jenny Rundberg	Vuxenpsykiatri Malmö / Trelleborg	Verksamhets- utvecklare	Malmö	Personligt möte / 53 min	4
	Per Granvik	Vuxenpsykiatri Malmö / Trelleborg	Verksamhets- utvecklare			
4	Karina Stein	Beroende- centrum Malmö / Trelleborg	Områdeschef	Malmö	Personligt möte / 44 min	5

Tabell 2: Respondenter

3.1.3 Intervjuer

Intervjuerna som genomfördes var av semistrukturerad karaktär, där ett visst antal teman med förutbestämda frågor ställdes till respondenten i form av en intervjuguide. Att följa en semistrukturerad karaktär på frågorna gjorde att följdfrågor kunde ställas vid behov samt att svaren från respondenten kunde bli mer utvecklade och detaljerade än om intervjun hade varit strukturerad (Bryman & Bell, 2017). Frågorna som ställdes var av öppen karaktär som möjliggjorde tolkningsutrymme av respondenterna och därmed ett detaljerat svar utifrån deras perspektiv och koppling till GDPR, samt medvetandegörandet av GDPR. Både tolkningar utifrån deras position, men också deras förståelse gällande GDPR i deras organisation möjliggjordes genom att ställa öppna frågor. Där vi inte uppfattade hur respondenten menade kunde även ett förtydligande ges på plats i form av fler följdfrågor ställdes.

Temana i intervjuguiden var baserade på frågeställningen och det teoretiska ramverket som används i studien. Detta för att respondentens svar skulle vara relevanta att analysera utifrån det teoretiska ramverket. Två huvudteman presenterades för respondenten: GDPR; och hur förberedelser inför GDPR ser ut, samt medvetenhet och medvetandegörande av GDPR. Efter varje intervju reviderades intervjuguiden om det ansågs gynna nästkommande intervju. Detta för att vissa ämnen kan ha uppmärksamats som vi inte tänkt på innan intervjun genomfördes.

Totalt genomfördes fyra intervjuer med fem intervjupersoner där alla intervjuer utom en intervju hölls som ett personligt/fysiskt möte. Två av respondenterna hade jobbat gemensamt med GDPR på deras avdelning och ville därför delta vid samma intervjutillfälle. Intervju två, hölls via Skype med en kamera igång för att efterlikna ett personligt möte så mycket som möjligt. Skype användes då respondenten satt på en annan ort, än vad vi gjorde. Via kamera och vid de personliga mötena, så kunde intervjupersonens kroppsspråk och ansiktsuttryck utläsas för att få en helhetsbild över intervjun och när det var läge att gå vidare med nästa fråga innan respondenten hunnit besvara frågan.

De personliga mötena hölls på respondenternas egna kontor eller konferensrum på respondenternas arbetsplats för att öka chansen till att intervjuerna skulle bli av, och underlätta för respondenten (Jacobsen, 2002). Via Skypemötet så upplevde vi inte någon förändring i kvalitén på intervjun jämfört med de intervjuer vi hade i ett personligt möte. Respondenten som deltog i Skypemötet gav diskuterande och uttömmande svar, precis som de övriga intervjuerna. Därför bedömer inte vi att denna intervjun har påverkats nämnvärt i avseendet att den var utförd på ett annat sätt än övriga intervjuer.

Innan intervjun startade gavs ett medgivande om att det var okej att spela in ljud för att säkerställa att citat blev korrekta och för att vi skulle ha möjlighet att vara lyhörda på vad respondenten sa och därmed kunna ställa bra följdfrågor (Jacobsen, 2002). Intervjuerna inleddes med frågor kring respondentens roll och position inom organisationen, samt hur länge respondenten hade varit verksam för att veta vilka frågor som kan ha blivit opassande att fråga då dessa inte var lämpade för respondenten. Respondenten blev också informerad om att anonymisering var ett alternativ, men ingen av respondenterna valde att hålla sig anonyma. Intervjuernas längd var mellan 36 till 53 minuter långa.

3.2 Analysprocessen

Efter avslutad intervju så transkriberades varje intervju i separata dokument (Jacobsen, 2002), dessa finns längst bak i appendix 2-5. Detta för att kunna säkerställa vad som sades under intervjun och kunna få med citat som är korrekta. Detta utan en möjlighet till misstolkning av respondenternas svar i presentationen av resultatet i empiriavsnittet. I transkriberingarna presenterades det som sades i inspelningarna ordagrant med undantag för plötsliga avbrott i meningar, eller otydligheter som inte kunde urskiljas från inspelningarna (Jacobsen, 2002). När transkriberingarna var klara skickades respektive till berörd respondent för att få möjlighet att göra ändringar om något hade blivit inskrivet eller tolkat på ett felaktigt sätt. Detta för att säkerställa att det som sades under intervjun, men även det material som analyserades, är baserat på vad som faktiskt kom fram i intervjun.

I nästa steg påbörjades ett kodningsarbete med kodord och tillhörande färg som transkriberingarna markerades med. Detta gjordes för att underlätta processen med att hitta relevant information till studien och för presentationen av resultatet (Jacobsen, 2002). Inledningsvis så försökte analysen hållas så öppen som möjligt, även under pågående intervjuarbete. Detta för att inte utelämna information som kunde bli relevanta för studien (Jacobsen, 2002). Kodningen baserades dels på teman som dels kom från intervjuguiden, men också på ämnen som vi, under intervjuerna hittat och ansåg vara viktiga för studien och dess resultat. Temana som användes var, informationssäkerhet, informationssäkerhetsmedvetenhet, medvetenhet, utbildning, säkerhetskultur, värderingar samt GDPR. Dessa teman bidrog sedan bland annat till rubriksättningen i empiri- och diskussionsavsnitten, samt även i viss mån det teoretiska kapitlet.

När kodningsarbetet var avslutat flyttades de markerade meningarna över till ett annat dokument för att sorteras in i de kategorier som tidigare hittats. Citaten matchades därefter ihop med teorier för att underlätta diskussionsavsnittet, som Jacobsen (2002) beskriver som att läsa citaten ur en ”teoretisk lins”.

Som sista steg i analysdelen, fetmarkeras de viktigaste citaten och flyttades in i analysavsnittet där de sattes ihop under respektive rubrik till en sammanhängande text. Där antingen citaten förblev just citat eller beskrevs utifrån vad som är sagt, sammanfört med andra respondenters svar. I detta avsnitt analyseras likheter och olikheter i respondenternas svar (Jacobsen, 2002). Citat som var extra tydliga eller påvisade ett visst fenomen valdes ut och skrevs in precis så som respondenten uttryckt sig i form av ett citat, medan övriga vävdes in i en sammanhängande text.

För diskussionen så skedde ett växelvist arbete med att läsa av och tolka in vad respondenterna sagt med vad teorin menar på, och hitta eventuella luckor som fanns mellan praktiken och teorin (Jacobsen, 2002).

3.3 Undersökningskvalité

3.3.1 Validitet och reliabilitet

För att mäta kvaliteten i studien, så tittade vi i enlighet med Jacobsen (2002) på intern- och extern giltighet/validitet. Där den interna validiteten syftar till att tittade på hur giltigt studiens resultat var (Jacobsen, 2002). Ett sätt vi gjorde detta på är att skicka våra transkriberingar av empiriinsamlingen till respondenterna, så att de fick ge feedback på att de kände igen sig i vad som stod. Den färdiga uppsatsen har även skickats ut till alla respondenter, dels av efterfrågan och intresse från respondenterna men också för att säkerställa att tolkningar som är gjorda i analysen inte är obefogade utan är i linje med empirin och det teoretiska ramverket. Genom att vi haft med transkriberingarna, intervjuguiden och beskrivit vårt metodval noggrant så kunde vi även använda oss av den externa validiteten. Där det handlar om överförbarhet och generalisering och att kunna återskapa studien igen (Jacobsen, 2002).

För att titta vidare på studiens tillförlitlighet, eller reliabilitet, så tar Jacobsen (2002) upp undersökningseffekter och kontexteffekter. Intervjueffekten som kan uppstå vid intervjuer är något vi har varit medvetna om inför intervjun. Vilket också gjort att vi försökt minimera effekten, genom att en utav oss höll i intervjun varpå den andra satt i bakgrunden och lyssnade, med undantag för följdfrågor som ställdes vid behov. Innan intervjun diskuterades även hur man på bästa sätt ställer frågor till intervjupersonerna samt när man kunde gå vidare i intervjun och påbörja nästa fråga. Med det sagt så kan vi inte garantera att någon påverkan på av intervjutillfället inte har skett, men medvetenheten kring den anser vi har givit oss kunskap om hur intervjueffekten, för att denna skulle kunna minimeras.

Kontexteffekter menar Jacobsen (2002) på att det finns två kontextuella sammanhang; naturlig eller artificiell. Den artificiella kontexten innebär att intervjun förekommer i ett ovant sammanhang för intervjupersonen. Medan den naturliga kontexten sker i ett sammanhang som är bekvämt och naturligt för respondenten. Den sistnämnda är något som vi försökte efterlikna så mycket som möjligt, så att inte intervjupersonen skulle påverkas av omgivningen eller val av plats för intervjun. Valet av intervjuplats baserades även på bekvämlighet och tid för respondenten så att inte vår intervju skulle störa deras dagliga arbete allt för mycket, och därför inte vilja medverka på grund av dessa faktorer.

Jacobsen (2002) tar även upp faktorer som ifall intervjun är planerad eller överraskande. Vid en överraskande intervju menar Jacobsen (2002) på att det är lättare att undersöka respondentens känslor och spontana åsikter. Men i denna studie så är syftet mer relaterat till att få saklig information gällande hur man medvetandegör GDPR inom organisationen. Vilket gör att en planerad intervju var att föredra (Jacobsen, 2002). Intervjutid och plats avtalades därför innan via mejl och intervjuguiden skickades ut till respondenten dagen innan intervjun hölls.

3.3.2 Etik

Vid studier behöver etiska aspekter tas upp för att säkerställa att fenomenet som undersöks är gjort på ett korrekt sätt. Jacobsen (2002) tar upp tre aspekter som är särskilt viktiga, nämligen; informerat samtycke, krav på privatliv och krav på att bli återgiven på ett korrekt sätt. För att säkerställa informerat samtycke i denna studie så hade vi i urvalsprocessen av respondenter

undersökt vilken typ av roll i organisationer som kan tänkas svara på våra frågor på ett informativt och givande sätt, detta bidrar alltså till att kompetensen uppfylls (Jacobsen, 2002).

Vidare så har respondenterna frivilligt ställt upp på förfrågningarna som skickades ut via mejl. Innan intervju så har respondenterna även fått information om vad intervju ska handla om för att säkerställ att de har en förståelse för vad vi skulle ta upp, samt kunna förbereda sina svar och ge respondenterna en möjlighet att skapa en förståelse för studien. Eventuella frågor som intervjupersonerna kan ha tänkas ha haft besvarades i den mån det gick via mejl eller vid intervjutillfället. Innan intervjutillfället så har frågorna noga utvärderats i aspekten hur känsliga frågor som ställts till respondenten.

Då vårt syfte inte är att undersöka respondentens känslor eller spontana åsikter, utan är mer ute efter saklig information hur någonting fungerar i en organisation, så klassade vi frågorna som mindre känsliga. Den allmänna påverkan på respondenternas privatliv blev därför liten (Jacobsen, 2002). Alla respondenter fick även valet av att vara anonyma innan intervjun, samt gav sitt samtycke till att ljud spelades in för att kunna säkerställa att det som sades återgavs korrekt. Många av respondenterna var även intresserade av att ta del av studien när den är klar vilket gör att vi gjort vårt yttersta för att återge och dra slutsatser kring det vi frågat om och inte dra slutsatser som inte det empiriska materialet givit oss.

3.3.3 Kritik

Urvalet av respondenter gjordes baserat på de kontakter vi hade tillgång till. Ett medvetet val var även att respondenterna behövde känna till vad GDPR innebar för deras verksamhet, men även inneha en viss översiktlig syn på verksamheten, alternativt en chefsposition. Därmed kan studien i viss mån kritiseras för att inte ett bredare spann av respondenter som deltog. Detta är dock något vi haft i åtanke vid analysen av vårt material och har därmed varit försiktiga med att inte dra slutsatser som inte vi kan säga något om med hjälp av de respondenterna vi haft. Vi ansåg dock att de krav som vi hade vid urvalet var nödvändiga för att kunna besvara vår frågeställning och har därmed varit till gagn för studiens slutsats.

Innan intervjuerna genomfördes så skickades intervjuguiden ut till respektive respondent. Vi ansåg att svaren vi var ute efter, inte var baserat på respondenternas individuella upplevelse av hur förberedelserna såg ut inom organisationen. Utan att frågorna vi ställde var mer av en faktabaserad karaktär, vilket gör att vi ansåg att svaren vi fick inte påverkades på ett sätt som var negativt för studien, utan snarare att vi fick genomtänkta svar som var relevanta och gjorde även att respondenten kunde förbereda sig och därmed inte blev överraskade och gav ett svar som inte var sanningsenligt. Dock är vi medvetna om att utskicket av intervjuguiden kan ha påverkat hur respondenterna svarade, men det är inget vi upplever försämrar studiens resultat.

Vi är även medvetna om att studien vi genomfört är en liten studie, så förväntningarna inför resultatet var inte att kunna dra generella slutsatser. Utan vi förväntade oss att förhoppningsvis kunna bidra med en annan vinkel på befintliga teorier, och kunna sätta ljus på de utmaningar som sjukvården och eventuellt andra myndigheter kan ställas inför, vid införandet av en större policyförändring.

4 Empiri

I följande avsnitt presenteras en analys av den insamlade empiriska data, baserat på de rubriker som återfinns i det teoretiska ramverket.

4.1 Empiriskt resultat

4.1.1 GDPR

Verksamhetsutvecklaren Karim på Unilabs, beskriver att Unilabs är i fasen att de skapar en GDPR organisation med bland annat en GDPR-officer och det kommer bli en egen organisation i organisationen. Även Region Skåne som är en stor organisation har skapat en struktur runt arbetet med GDPR enligt Kanslichefen på Region Skåne, Olivia, i form av att varje verksamhetsområde har en kontaktperson. Sedan har även varje enhet inom verksamhetsområdet en kontaktperson och kontaktpersonerna både på enhets- och verksamhetsområdesnivå ansvarar för att driva frågan inom sitt område. Dock nämner Olivia att enhets- och verksamhetschefen är de som ser till att arbetet med GDPR blir gjort, eftersom de har lite mer kompetens.

För att vad GDPR gör är att sätta ljuset på den svaghet som finns i organisationen, kring kompetensen, kring de här frågorna, hur vi faktiskt gör och i och med att folk nu har entydig medvetenhet, brist i kompetens och brist i medvetenhet får en väldigt tydlig påverkan på organisationen om man skulle börja granska oss med GDPR glasögon. (Olivia, Kanslichef Region Skåne)

Hon fortsätter beskriva att GDPR har lyft på locket på en stor frågeställning kring arkivering och gallring som en del av stödarbetet för GDPR. Hon påpekar att de saknar utbredd kompetens inom just arkivering och gallring, samt att de problem som GDPR sätter ljuset på inom verksamheten, påverkar personalen starkt och skapar stress i verksamheten.

Ett problem som Olivia även nämner är att, när de kontaktar de som står som kontaktpersoner för förteckningar inom organisationens PUL-register, vilka kan ha angetts till kontaktpersoner exempelvis när en forskningsstudie inletts. Sedan har studien dragit ut på tiden och kontaktpersonerna är inte längre ansvariga för det registret. Kontaktpersonerna ställer sig då frågande till hur de fortfarande kan stå kvar som kontaktpersoner när de nu kontaktas av Olivia och hennes team.

Karina, områdeschef på Beroendecentrum i Malmö och Trelleborg, beskriver att på Beroendecentrum är det medarbetare med stora patientvolymen på kort tid och med snabba möten, som kommer påverkas mest av GDPR. Hon menar att de behöver ha möjlighet att kontrollera om alla patienter kommit till mottagningen, i de system som medarbetaren arbetar i, vilket det tyvärr inte finns någon funktion för. Där ser Karina att kraven för GDPR inte stämmer överens med hur medarbetarna måste arbeta med patientgrupperna. Då behovet för att kunna få en överskådlig vy om en patient har uteblivit, eftersom uteblivet besök kan innebära att något allvarligt har hänt, inom hennes patientgrupp.

I motsats till de problem som respondenterna uttrycker, så ser verksamhetsutvecklaren för psykiatri i Malmö och Trelleborg, Jenny, GDPR som någonting positivt. Då förändringarna som kommer komma med GDPR, ifrågasätter om insamlad information verkligen behövs och var den ska förvaras, samt att bara samla in det som verkligen behövs och reflektionerna kring detta. Hon nämner att det kanske är ett litet 'Wake up call' i och med detta.

4.1.2 Informationssäkerhet

GDPR har onekligen påverkat alla organisationer som behandlar personuppgifter, inte minst skapar förordningen oordning inom sjukvården, där personuppgifter behandlas i allra högsta grad. Kanslichefen Olivia och verksamhetsutvecklaren Jenny menar båda på att en brist som belysts i arbetet med GDPR, har varit den om informationssäkerhet där befintliga system är svåra att använda för den tänkta verksamheten. Detta är något som majoriteten av respondenterna är överens om. Däremot är Olivia tacksam över att problemen har kommit ut i ljuset då detta är något som hon ansåg behövdes.

Det har väckt frågan kring arkivering och gallring som ligger i kanslifunktionen. Vilket gör att vi nu har en möjlighet att hoppa vidare med de frågorna, från att det tidigare har varit lite styvmodigt behandlat område. (Olivia, Kanslichef Region Skåne)

Fyra av fem respondenter svarade att de system som är tillgängliga idag, inte är tillräckliga. Områdeschefen Karina, menade på att personalen behöver komma på egna ad hoc lösningar för att kunna utföra det dagliga arbetet, exempelvis externa listor över patienter som ska komma in samma dag. Dessa listorna sparas inte på säkra e-platser, vilket gör att de personuppgifter som finns på listorna inte överensstämmer med kraven från GDPR som exempelvis kravet kring pseudonymisering.

Per, även han verksamhetsutvecklare för psykiatri i Malmö och Trelleborg, menar på att den största utmaningen kommer ligga högre upp i organisationen. Att det är de tekniska lösningarna som kommer spela roll för hur väl sjukvården kommer hantera GDPR. Det är även något som alla respondenter inom Region Skåne nämner, att det är problem med befintliga system för att de inte uppfyller kraven för de dagliga arbetsuppgifterna, vilket Jenny och Per tryckte extra mycket på under deras intervju. Per nämner att det är en fråga som behöver drivas högre upp i organisationen.

Olivia beskriver vidare att en stor inventering har pågått i hela Region Skåne om vilka system och register som finns, och att medarbetare har blivit ombedda att städa i sina datorer efter personuppgifter som inte ska ligga där. Dock menar hon på att, på grund av att Region Skåne är en jättestor organisation, med 14 000 anställda i den delen där Olivia jobbar, så vet de inte ens hur mycket information de förväntas få in. Olivia betonar att det finns en stark vilja att göra rätt bland medarbetarna och att många frågor har uppkommit i och med inventeringen om hur medarbetarna ska gå tillväga för att göra rätt och lägga informationen på ett korrekt och skyddat ställe i datorn. Verksamhetsutvecklaren Jenny berättar att i samband med övergången från pappersjournalen till digital journalföring har det skapat en uppfattning hos anställda att datorn generellt är en säker plats, och hon benämner att datorn ibland kan användas som en "dumpningsplats". Hon berättar vidare att arbetet med GDPR har ifrågasatt det befintliga beteendet:

Till att nu GDPR säger att, det ska vi inte alls [använda datorn som en dumpningsplats], utan nu ska det rensas nu ska ni bara ha det ni måste ni ska verkligen ifrågasätt om ni verkligen behöver den här informationen och var den förvaras, så kanske lite så 'Wake up call' i det. (Jenny, Verksamhetsutvecklare Psykiatri Malmö och Trelleborg)

Områdeschefen Karina, tar upp en aspekt kring just digitaliseringen av sjukvården, med att det finns även nackdelar med digitaliseringen och att den kan komma missbrukas precis som Jenny beskriver ovan. Även om detta kan ske oavsiktligt.

Verksamhetsutvecklaren Karim, tror att hanteringen av persondata, som exempelvis vid faxning, som är en mer slentrianmässig arbetsuppgift, kan bli en av de stora förändringarna. Det är arbetsuppgifterna som sitter i ryggmärgen som kan bli den stora förändringen. Karina går även in på det faktum att man är väldigt vanestyrd vilket är ytterligare en faktor till varför dessa förändringarna kommer bli stora i hur man jobbar med systemen. Olivia tar dessutom upp att gamla rutiner ofta appliceras även på nya system:

[...] i det gamla sättet för att det var så vi behövde göra med system X men nu har vi system Y, då måste vi jobba med systemet för att förenkla arbetssätten och säkerställa att det flyter på smidigt och tyvärr är det så att man tar arbetssätten från det föregående systemet och försöker lägga det ovanpå det nya så resulterar det i att man gör en extra kringelkrok. (Olivia, Kanslichef Region Skåne)

Detta i sig kan resultera i att informationssäkerheten kompromissas för att systemen inte brukas som de bör, och för att det inte finns en förståelse för hur systemen ska användas framförallt när en ny lagstiftning kan komma att påverka hur personal lägger in personuppgifter. Olivia berättar att IT-systemen idag inte är tillräckligt bra och att det inte finns nog med säkra lagringsplatser för att kunna nå upp till vad GDPR kräver. Karina ser två lösningar på denna problematik, dels införandet säkra e-platser att lagra informationen på men också genom att utveckla system som är anpassade för den dagliga verksamheten så att inte onödiga listor och rutiner behöver tas till för att utföra arbetet och därmed göra kompromisser vad gäller dataintegritet och informationssäkerheten, vilket sker i dagsläget.

4.1.3 Informationssäkerhetsmedvetenhet

När det kommer till informationssäkerhetsmedvetenhet så menar verksamhetsutvecklaren på Unilabs, Karim att medarbetarna har ett personligt ansvar att vara en del av processerna på arbetsplatsen samt skriva avvikelser för att uppmärksamma fel. Per, verksamhetsutvecklaren, är av liknande åsikt när det kommer till att hålla sig uppdaterad både vad gäller information som kommer ut på intranätet samt genomföra obligatoriska utbildningar i deras utbildningsportal, där även cheferna kan se om medarbetare inte gjort det som åligger dem att göra.

4.1.3.1 Medvetenhet

Kanslichefen Olivia menar att de inom hennes verksamhet har kunskap om arkivering, men i och med GDPR, så öppnas en viss osäkerhet upp kring vad som gäller. Men hon ser även en möjlighet att se över hur de hanterar information, samt arkivering och gallring av information förknippat med GDPR.

Både Olivia och verksamhetsutvecklarna Jenny, Per och Karim menar att förändringarna kommer ligga i ökad medvetenhet kring vilka personuppgifter som sparas, varför de sparas,

sekretess samt hur patientdata skickas till andra vårdgivare. Per menar även att ökad medvetenhet kan leda till en större försiktighet i hur känsliga personuppgifter hanteras. Olivia anser även att medvetandegörande av vad GDPR innebär är en del av sjukvårdens uppdrag:

Det medvetandegör det här att det är en del av vårt uppdrag, att visa på att vi tar ansvar för dels för vår roll som myndighet men också att de personuppgifter som finns hos oss är trygga och att vi faktiskt kan berätta varför vi har de personuppgifter vi har och vad vi gör med dem. [...] tidigare kanske har kunnat sopa in i hömet lite behöver dras fram nu i ljuset och verkligen säkerställa att vi förstår varför vi gör det. (Olivia, Kanslichef Region Skåne)

Verksamhetsutvecklaren Karim menar att medvetenheten kan skilja beroende på vem du pratar med. Viss personal har kanske inte förstått omfattningen av GDPR för att kunskapen inte finns om dess innebörd fullt ut i organisationen. Han menar även att de inom Unilabs medvetandegör ämnet för medarbetarna. Områdeschefen Karina tar även upp detta när hon syftar till att hon, ganska tidigt, uppmärksammade att en lag skulle komma.

Olivia ser det som att de, bit för bit försöker sprida medvetenheten om GDPR, men det finns ingen statistik på hur många man nått ut till och om de verkligen lyckas nå ut till alla 14 000 medarbetare. Men hon ser det positiva i att de har kontaktpersoner inom GDPR nätverket som har till uppgift att informera kollegorna på sina respektive enheter.

Strukturen för hur organisationer medvetandegör både lagar, policys och förändringar kan se ut på olika sätt beroende på hur organisationen är uppbyggd. Både områdeschefen Karina och verksamhetsutvecklaren Per pratar om att Region Skåne är en linjeorganisation där information går både ner och upp längs denna linje. Där nämner Karina även att informationen kommer från arbetsgruppen för GDPR till ledningsgruppen där chefer har informerats och fått i uppdrag att informera sina medarbetare om GDPR samt om att det ska städas kring hur personuppgifter hanteras i deras verksamhet. Alla respondenter inom Region Skåne pratar om inventering av personuppgifter och ser det som en del i att medvetandegöra hur de hanterar personuppgifter. Per menar att en utmaning ligger i att nå ut med informationen till alla deras medarbetare.

Karim, verksamhetsutvecklaren, nämner att han genomför intervjuer med leverantörer, för att jämföra den medvetenhetsgrad med vilken nivå Unilabs ligger på och hur leverantören jobbar utifrån GDPR. En del i deras arbete i att medvetandegöra GDPR. Det hjälper dem i frågan hur de kan ställa sina förväntningar jämfört med leverantörens medvetenhet kring GDPR.

Vidare nämner Karim hur de har protokoll att följa vid deras APT (arbetsplatsträff). Där bland annat informationsansvar ingår, här tas även avvikelser upp till diskussion under träffarna. Men han menar också att informationsansvar ingår i introduktionen för medarbetare, där medarbetaren medvetandegörs om vilka regler och lagar som finns och ska följa. Verksamhetsutvecklaren Jenny tror att arbetet med GDPR och att medvetandegöra förordningen kommer bli en kontinuerlig process inom verksamheten. Liknande menar kanslichefen Olivia när hon nämner förändringskommunikation och medvetandegörande:

Ja, alltså om man säger förändringskommunikation om du ska medvetandegöra nånting eller nånting ska fastna och sånt, så säger man att det måste repeteras minst sju gånger. (Olivia, Kanslichef Region Skåne)

4.1.3.2 Utbildning

Både verksamhetsutvecklarna Jenny och Karim samt kanslichefen Olivia nämner att utbildning kring GDPR ligger i planeringen, Jenny nämner vidare att det ska finnas som en webb-utbildning. Olivia förklarar att en del av utbildningsmaterialet är gemensamt för hela Region Skåne samt att det finns en funktionsbrevlåda dit frågor kan skickas och att de tar hjälp av det regionala projektteamet som finns. När det gäller utbildning i informationssäkerhet nämner Olivia att det finns, men att det är tydligt att den är okänd för medarbetarna i organisationen. Däremot så tar områdeschefen Karina upp att det har skett utbildningar och informationsmöten för områdeschefer och enhetschefer kring GDPR. Vidare nämner Karim att de inom Unilabs, har med sig erfarenhet från tidigare förändringar i organisationen. Både när det gäller införandeprocessen, processen för utrullning av utbildning och information till medarbetarna.

Både Olivia och Jenny pratar om att GDPR utbildningen bör vara en del av introduktionen för nya medarbetare. Olivia beskriver även att de som arbetat ett tag men är ny på arbetsplatsen kanske inte har stött på GDPR tidigare och behöver då få utbildning i det. Per nämner även detta, då han menar att genom medvetandegörandet av GDPR så får medarbetare information hur de ska hantera den känsliga informationen.

Olivia pratar om att när utbildningen väl kommer så finns ett behov att titta på vilka som ska prioriteras när det gäller utbildningsinsatsen och där ha med de grupper som har GDPR centralt i sina arbetsuppgifter. Hon nämner vidare att en del i prioriteringen beror på att utbildning är en kostnad för verksamheten och det speciellt när man inom sjukvården är underbemannade på alla positioner.

4.1.4 Säkerhetskultur

Verksamhetsutvecklaren Karim, pratar om att förståelsen, hos anställda, för GDPR kommer bli den svåraste utmaningen enligt honom. Han tar vidare upp att det är viktigt för honom att förmedla var Unilabs står i frågan kring GDPR i både mötena med medarbetare men också med såväl interna som externa kunder och företagets leverantörer. Både Karim, Karina och Olivia menar alla på att GDPR behöver bli en naturlig del av det vardagliga arbetet. Jenny menar att GDPR kommer bli en kontinuerlig process. Kanslichefen Olivia tar även upp att för att de ska kunna följa sitt myndighetsansvar och behålla den transparens som behövs. Så behöver kraven för GDPR appliceras på ett sätt som gör att det blir en naturlig del av vardagen och organisationskulturen. Hon uttrycker sig vidare som:

Ja, alltså GDPR har blivit liksom, det har blivit en slogan. (Olivia, Kanslichef Region Skåne)

Karim menar vidare på att han tror att GDPR kommer bli ett "culture behaviour" som är något de jobbar med inom Unilabs och implementera GDPR i deras "mission motto-mantra" och "culture building behaviours" som de arbetar med kontinuerligt i det dagliga arbetet samt runtom i verksamheterna. Områdeschefen Karina menar även på att mycket är upp till enhetschefen att informera medarbetarna om hur informationssäkerhet ska implementeras och hur medarbetarna ska tänka gällande informationssäkerhet i deras dagliga arbete. Verksamhetsutvecklaren Per trycker dessutom på att medvetenhet kring hur och vilka personuppgifter ska lagras är något som medarbetaren själv måste fundera över samt på varför uppgifterna behövs. Om enhetscheferna, som Karina beskriver, kan lyckas med arbetet att informera om personuppgifter, kan chanserna öka för att medarbetarna själva börjar reflektera över personuppgifterna och därmed lyckas implementera tankesättet i deras vardag på arbetsplatsen.

4.1.4.1 Värdegrund

Verksamhetsutvecklaren Karim diskuterar att han inte anser att utbildning är nog för att få full förståelse för hur förordningen kommer påverka olika företag. Han tar upp vikten av att prata om GDPR även med släkt och vänner, då han inte anser att ett företagsperspektiv är nog i frågan. För att uppnå den totala förståelsen för hur GDPR kommer påverka företagen behöver även frågan lyftas utanför företaget, då det egentligen är individen som förordningen faktiskt påverkar. Olivia, kanslichefen på Region Skåne, pratar vidare om att, för att uppnå en utbredd medvetenhet kring GDPR, så behöver GDPR genomsyra arbetsuppgifter och de dagliga rutinerna, så att GDPR jobbas in i värdegrundsarbetet. Hon påpekar att detta är ett traggligt arbete som kräver fokus under lång tid tills dess att fokus finns mer naturligt i arbetsuppgifterna. Hon beskriver vidare:

Så det är ju egentligen den långsiktiga målsättningen är ju att det är lika naturligt som det är att andas och att vi sköter vår data. (Olivia, Kanslichef Region Skåne)

Per, verksamhetsutvecklaren inom psykiatri, diskuterar den största förändringen som han ser det, nämligen ökad medvetenhet hos personalen. Områdeschefen Karina pratar även om värdegrundsarbetet som har med personlig integritet att göra, där hon gör kopplingar till arbetet med GDPR. Karim diskuterar vidare på detta spåret och hur personuppgifter uppfattas inom sjukvården:

[...] GDPR har ingen patientrelation utan den har en personrelation och jag tror det är där som den största förändringen ligger att vi ser inte kanske alltid personen, vi ser patienten. (Karim, Verksamhetsutvecklare på Unilabs)

Karina berättar att det är lätt att skapa sig en referensram där det anses vara okej att arbeta på ett sätt där exempel externa listor används, som inte är godkända ur ett GDPR-perspektiv. Hon menar vidare på att denna referensram inte är accepterad då det handlar mycket om de värderingarna som de anställda har. Hon tar vidare upp ett exempel på detta nedan, och berättar att hon jobbat länge med tungt narkotikaberoende och har reflekterat kring den stigmatiserade grupp hennes avdelningar hanterar, samt alla människors lika värde:

[...] då tänker jag, nä, ja... räcker det när man jobbar med en heroinberoende kvinna, som är prostituerad och misshandlad, asså räcker det att man säger att alla har lika värde är det tillräckligt? För oss är det också viktigt att veta att vi jobbar med en väldigt stigmatiserad grupp, det är inte okej att ha listor till exempel, [...] det är väldigt integritetskränkande och vi måste få in det i vårt tänkande, vi måste arbeta med dem frågorna. (Karina, Områdeschef på Beroendecentrum i Malmö)

Hon reflekterar även över patientflödet, och de patienter som är heroinberoende om huruvida det är okej att ha sitt namn med på en lista över dagens patienter, och ställer sig själv frågan ”hade jag velat ha mitt namn på en sådan lista?”. Karina uttrycker även att det är en stor utmaning för personalen men också i viss mån för chefer att förstå vad en personuppgift är och hur viktigt integritetsskyddet är. Även kanslichefen Olivia, ser medvetenheten som en jättestor utmaning där hon menar på att eldsjälarna inom organisationen som brinner för frågorna är mycket viktiga och kan hjälpa till att driva frågorna inom organisationen. Karina anser dock att GDPR har skapat en högre medvetenhet kring integritetsfrågor inom hennes organisation. Olivia påpekar återigen att medvetenheten bör byggas in i ryggraden och att det ska innefattas i att göra allt för patienten, men att medvetenheten inte behöver ligga längst fram i pannan.

Hennes förhoppning är att när dammet har lagt sig, så ska det dagliga arbetet inte påverkas allt för mycket. Men då sjukvården finns till för medborgaren och bär ett myndighetsansvar så ställer hon sig dock frågande till hur man ska lyckas med generell medvetenhet:

Hur man nu ska göra det, jag vet inte, Matrix. (Olivia, Kanslichef Region Skåne)

5 Diskussion

5.1 Informationssäkerhet

Enligt Flowerday och Tuyikeze (2016) är det viktigt att ta hänsyn till såväl interna som externa faktorer vid skapandet av en säkerhetspolicy. När det kommer till den externa bedömningen så anser vi att GDPR bör vara en sådan faktor. Då GDPR påverkar sjukvården till den grad att den måste tas i beaktning för att sjukvården ska kunna fullfölja sitt myndighetsansvar. När det gäller de interna faktorerna så blir det tydligt att respondenterna från Region Skåne anser att deras IT-system är otillräckliga för att kunna utföra det dagliga arbetet på ett GDPR-kompatibelt sätt. Som Shoniregun et al. (2010) beskriver så bör organisationer vara följsamma när det kommer till informationssäkerhet, vilket vi bedömer inte är fallet i Region Skåne när det kommer till GDPR, utifrån de respondenter vi talat med.

Enligt respondenternas beskrivningar kring den befintliga säkerheten och medvetenheten kring vilka system som finns och hur de används. Men också osäkerheten kring vilka register som finns och inventeringen av information på personliga datorer, så tolkar vi att Region Skånes system för närvarande inte är följsamma som Shoniregun et al. (2010) föreslår att organisationer bör vara. Shoniregun et al. (2010) menar även att policyn säkrar hur patientinformation hanteras samt patienters integritet och konfidentialitet i enlighet med lagar och regler, vilket är ännu en anledning till att organisationer bör sträva mot att vara följsamma när det gäller informationssäkerhet. Risken är även att informationssäkerhetspolicyn, som enligt Socialstyrelsen ska finnas på varje vårdenhets (HSLF-FS 2016:40), blir otillräcklig precis som Flowerday och Tuyikeze (2016) menar på. Då policyn inte får stöd från de anställda i det avseendet att de inte vet vad som gäller alternativt inte förstår varför en policy finns.

McIlwraith (2016) beskriver även att personal behöver ha rätt kompetens för att klara av de dagliga arbetsuppgifterna. Detta är något som vi ser en brist i när det kommer till systemen och kompetensen kring uppföljning av standarder och policys i de system som respondenterna i Region Skåne arbetar i. Vi uppfattar det som om att det finns en viss medvetenhet främst hos cheferna i organisationen, men att det, trots detta förekommer bristfälligt beteende i hur dagligt arbete utförs bland andra medarbetare, som inte är i linje med GDPR. Oavsett om detta är något som sker oavsiktligt eller som sker för att en arbetsuppgift ska kunna utföras överhuvudtaget, så följer det inte de standarder som bör finnas kring informationssäkerhet. Konsekvenserna med att inte göra något aktivt åt beteenden som inte är "säkra" ur ett informations-säkerhetsperspektiv, är att andra beteenden kan bli accepterade och kan ha varit pågående under en längre tid. Detta kan leda till stor skada för organisationen i sin helhet precis som studien från HIMSS (2017) trycker på.

Det finns även en risk när en organisation blir för insnöade på att det är systemen som kräver förbättringar, precis som två av verksamhetsutvecklarna, Jenny och Per, tryckte på extra mycket på i sin intervju. Att organisationen glömmer bort att informationssäkerhet inte bara handlar om säkra system utan även är ett 'Peoples issue' som AlHogail (2015) menar på.

5.1.1 Säkerhetsbeteende

På grund av de befintliga problemen med att lagra och använda systemen på ett lämpligt sätt utifrån den dagliga verksamheten, så riskerar informationssäkerheten att kompromissas och personuppgifter kan komma att behandlas på ett felaktigt sätt. Framförallt när ad hoc lösningar används för att komplettera de befintliga systemen. Såsom externa listor som områdeschefen Karina beskriver används för att hålla koll på dagens patienter i patientflödet.

Karina beskriver ett beteende där personalen skapar sig en referensram där det är mer eller mindre okej att äventyra patientens integritet och konfidentialitet, genom att hantera patientens personuppgifter på externa listor utanför säkra lagringsplatser. Ett sådant beteende på en arbetsplats kan bidra till att andra beteenden kring informationssäkerhet kan bli accepterade trots att, de ur ett informationssäkerhetsperspektiv, är felaktiga.

Ramverket som Alfawaz et al. (2010) föreslår för att identifiera hur de anställdas kunskap, färdigheter och deras uppfattningar kring informationssäkerhet ser ut, kan bidra till ett arbetsätt som blir informationssäkert. Även Frye (2007) föreslår att personal bör få information och vägledning om vilket beteende som är lämpligt eller ej ur ett informationssäkerhetsperspektiv. Även Shoniregun et al. (2010) trycker på att det är viktigt att göra personalen medveten om säkerhet och integritetsskydd för att säkerställa att säkerhetspolicyn följs. Vi kan utläsa från respondenterna i Region Skåne, att detta är något som de vill uppnå, framförallt när Kanslichefen Olivia betonar att det finns en stark vilja att ”göra rätt”. Vår uppfattning är dock att organisationen inte är där ännu, då frågor om befintliga system behöver tas högre upp i organisationen för att få förbättringar i befintliga system, alternativt hitta andra lösningar med säkra lagringsplatser, innan de når dit fullt ut.

Precis som områdeschefen Karina och verksamhetsutvecklaren Jenny beskriver, kan digitaliseringen komma att missbrukas och handlingar kan ske som bryter mot säkerhetspolicyn samt riskerar informationssäkerheten, även om detta sker oavsiktligt. För att inte riskera att göra fel, men även för att använda systemen på ett korrekt sätt så bör enligt Shoniregun et al. (2010) kraven för GDPR läggas in i organisationernas säkerhetspolicy för att fastställas och så att personuppgifterna säkras upp. Det blir dessutom tydligt att det är oerhört viktigt att informera personalen som hanterar personuppgifter, att förstå hur uppgifterna ska behandlas.

Katsikas (2000) betonar att medvetenheten kring informationssäkerhet inom sjukvårdsenheter blir omöjlig att bortse ifrån i och med den tekniska miljön sjukvården arbetar inom. När Jenny beskriver att synen på datorer som lagringsplatser, och att de används som en dumpningsplats, blir det tydligt att det inte finns en tillräcklig medvetenhet kring hur sjukvårdens system och hur de digitala hjälpmedlen ska användas.

Det Kanslichefen Olivia, nämner med att gamla processer används i nya system. Det kan även bli ett problem för säkerheten i systemen när man håller kvar vid gamla sätt att utföra ett arbete på, istället för att anpassa sättet att jobba på till det nya systemet. Verksamhetsutvecklaren Karim och områdeschefen Karina betonar dessutom det vardagliga arbetet som slentrianmässigt och att människor är vanestyrda. Detta kan skapa problem vid införandet av en ny säkerhetspolicy som Sujana (2018) beskriver, ett vanestyrt arbete kan ses som en risk i samband med en policyförändring som organisationer behöver ta hänsyn till. Precis som Knapp et al. (2009) beskriver är det därför viktigt att friska upp minnet av säkerhetspolicyn för att minska risken för att göra fel. De menar även på att det är en av de största utmaningarna med att en

implementation av en säkerhetspolicy. Vilket är något som måste finnas i åtanke när GDPR ska implementeras i säkerhetspolicyn.

5.2 Informationssäkerhetsmedvetenhet

När det kommer till informationssäkerhetsmedvetenhet pratar verksamhetsutvecklarna Karim och Per om det personliga ansvaret kring processer och att hålla sig uppdaterad kring detta. Vilket även kan tolkas in i det Knapp et al. (2009) skriver om tankesättet kring informations-säkerhet samt uppföljning av informationssäkerhetspolicy och att integrera dessa i den dagliga verksamheten. Samtidigt följer det vad McIlwraith (2016) skriver om vägledning för att förstå informationssäkerhet och medvetenhet om personligt ansvar som anställd samt vikten av medvetenhet om vad man som medarbetare kan göra för att öka informationssäkerheten.

Olivia, kanslichefen i Region Skåne pratar om både kunskap inom vissa delar, men att GDPR innebär en möjlighet att se över hur man hanterar information. Men också hur delar inom arkivering och gallring som är förknippat med GDPR blir en möjlighet för organisationen. Kunskapsdelen kan kopplas till det som tidigare nämnts av McIlwraith (2016) angående vägledning för att hjälpa medarbetarna att göra rätt. Även Katsikas (2000) tar upp vikten av medvetenhet inom hälso- och sjukvård på grund av den ytterst känsliga information som hanteras. Wiles et al. (2012) påpekar också vikten av medvetenhet för att skydda känslig information, vilket även kan ses vara viktigt i det Olivia nämner.

Shoniregun et al. (2010) beskriver att en säkerhetspolicy är viktig för att behandla patientinformation och säkra patienters integritet i enlighet med lagar och regler. Vilket vi kan se i att verksamhetsutvecklarna både inom Region Skåne och på Unilabs samt kanslichefen Olivia påpekar att förändringar kommer att ske i hur personuppgifter hanteras. Men även när Per nämner att medvetenheten kan leda till större försiktighet i hur personuppgifter behandlas, vilket även kan ha en grund i det He och Johnson (2017) beskriver med att exempel på att säkerhetsincidenter bör inkluderas i säkerhetsutbildningen. Vidare pratar Olivia även om Region Skånes uppdrag och ansvar som myndighet att medvetandegöra GDPR samt hur de behandlar personuppgifter inom organisationen. Här är Olivia överens med litteraturen som beskriver att alla medarbetare behöver medvetenhet på grund av sjukvårdens mer tekniska miljö (Katsikas, 2000), men även att en del kan vara att påverka organisationskulturen samt ha säkerhetstänket med i det dagliga arbetet för att öka medvetenheten bland medarbetarna (Wiles et al., 2012).

Alla respondenter i Region Skåne pratar om hur inventeringen av personuppgifter är en del i att medvetandegöra hur de hanterar personuppgifter och några nämner hur informationen om GDPR har gått i deras linjeorganisation uppifrån och ner. Delar av detta kan ses i det som skrivs om att medvetenhetsprogram inkorporerar organisationens policys för hur känslig information säkras (Wiles et al., 2012), men även det McIlwraith (2016) skriver om att medvetenhetsprogram och utbildning som används ska vara godkänt av organisationens ledning.

5.2.1 Utbildning

Både Olivia, Per, Jenny och Karim pratar om att GDPR behöver vara en del i introduktionen för nyanställda, vilket även litteraturen tar upp i form av Wiles et al. (2012), nämner att nyan-

ställda behöver en bra grund för att klara sina arbetsuppgifter, förstå och göra rätt när det gäller att skydda känslig information. Även Mehraeen et al. (2016) visar liknande resultat med utbildning för att veta hur patientinformation ska skyddas. Informationssäkerhetsmedvetenhet ses även vara en grundläggande del för att uppnå effektiv säkerhetshandling i en organisation, men är ensamt inget universalmedel (Frye, 2007).

Olivia nämner hur Region Skåne kommer behöva göra prioriteringar när utbildningen väl startar, utifrån vilka grupper som har GDPR centralt i sina arbetsuppgifter och att dessa prioriteringar beror på kostnader samt underbemanning. Även om Ghazvini och Shukur (2017) nämner att träningsprogram fokuserar på vad organisationen behöver och dess uppdrag, så nämner ingen litteratur att prioriteringar ska göras pga. kostnader och bemanning. Däremot lägger Katsikas (2000) vikt vid att ha tillräcklig medvetenhet och utbildning inom hälso- och sjukvårdssektorn. McIlwraith (2016) menar att om de som behöver det inte utbildas så ska det inte vara en överraskning om de begår misstag på grund av okunskap. Dock kan prioriteringarna som Olivia nämner ses i den statistik som MSB (2015) har tagit fram, där dubbelt så många procentuellt sett bland sekreterare och administratörer gått kurs i informationssäkerhet jämfört med sjuksköterskor. Men samtidigt skulle de låga procentsatserna kunna härledas till den underbemanning som Olivia pratar om.

Ghazvini och Shukur (2017) beskriver att en del i ett långsiktigt medvetenhetsprogram är att ha processer och resurser på plats. Detta kan till viss del, hittas hos Unilabs när Karim nämner att de har med sig erfarenhet från tidigare förändringar med införandeprocess samt process för utrullning av utbildning och information till anställda.

5.2.2 Medvetenhet

Av de svar vi fått av respondenterna så tolkar vi att respondenterna är medvetna om GDPR och informationssäkerhet. Men att det saknas en utbredd medvetenhet bland medarbetare eftersom det talas om listor som inte är godkända samt om utbildningar i informationssäkerhet. Olivia säger att man inte känner till utbildningen som finns tillgänglig i organisationen. Avsaknaden av utbredd medvetenhet skiljer sig från statistiken från USA som talar för att 87 procent får utbildning årligen (HIMSS, 2017), vilket vi inte har fått uppfattningen om är fallet enligt Olivia när det gäller informationssäkerhet, då hon nämner att det saknas utbredd kompetens i arkivering och gallring som är en del i GDPR. Vi tolkar det som att de som är chefer och verksamhetsutvecklare har i sin roll ett större ansvar att hålla sig uppdaterade och medvetna vad gäller lagändringar och informationssäkerhet, eftersom medvetenhet och erfarenhet av kontrollarbete samt incidenthantering är kopplat till ledningsansvar och kompetens (MSB, 2015). I de beskrivningar som respondenterna ger så uppfattar vi att chefer inom Region Skåne har en högre medvetenhet än övriga medarbetare, då utbildningar och informationsmöten gällande GDPR har varit mer riktade åt att utbilda cheferna i organisationerna, och att större ansvar läggs på att cheferna informera övriga medarbetare. Dock beskriver respondenterna att det inte finns något sätt att säkerställa att alla verkligen mottagit information kring GDPR och därmed gjorts medvetna.

Att genom medvetenhetsprogram om informationssäkerhet, få möjlighet att implementera säkerhetstänket i organisationskulturens värderingar. Detta kan göras via ett program där upprepning av information, sker sju gånger vid sju olika tillfällen, på sju olika sätt (Wiles et al.,

2012). Vilket återspeglas i det Olivia nämner om förändringskommunikation och att medvetandegöra saker, så behöver detta repeteras minst sju gånger. Kopplingen till implementation i organisationskulturen kan återspeglas när Jenny nämner att hon tror att medvetandegörande av GDPR kommer bli en kontinuerlig process.

5.3 Säkerhetskultur

Vi har kunnat se att flera respondenter anser att GDPR behöver bli en naturlig del i arbetet och att det kommer vara en kontinuerlig process, vilket stämmer väl överens med det AlHogail (2015) skriver om att kulturen behöver stödja säkerhetstänk vilket gör det lättare för medarbetare att jobba med detta tänk i sin vardag. Informationssäkerheten blir effektiv när medarbetare har förståelse och acceptans (AlHogail, 2015). Olivia pratar om att GDPR har blivit en slogan, detta kan ses som en process för att hantera förändringen och ger organisationen möjlighet att optimera möjligheterna för att skydda information i organisationen (Frye, 2007). Samtidigt kan detta med slogan ses som ett sätt att skapa medvetenhet bland medarbetarna om att skydda personuppgifter och genom att tas upp på möten, ge medarbetarna kunskap samt ingå i organisationens mål, vara till hjälp för att skapa en säkerhetskultur, vilket Hayden (2017) även påpekar i sin artikel.

Verksamhetsutvecklaren Karim pratar både om hur viktigt han anser det är att förmedla vart Unilabs står gällande GDPR både inom organisationen och till kunder och leverantörer, samt hur han det kommer implementeras i deras organisationskultur. Detta stärks av det Hassan och Ismail (2016) beskriver i sin artikel om medvetenhet och attityd hos medarbetare, samt vikten av att belysa både medvetenhet och beteende när det kommer till säkerhet i informationssäkerhetskulturen. Metalidou et al. (2014) och AlHogail (2015) stämmer även in om detta med kultur och säkerhetsmedvetenhet.

Malcolmson (2009) skriver om hur säkerhetskulturen kan påverka säkerheten i en organisation, detta stämmer överens med Karinas svar om enhetschefens ansvar kring att informera om och implementera informationssäkerhet i det dagliga arbetet. Vilket vidare även stöds i litteraturen av AlHogail (2015) och Ramachandran et al. (2008) att säkerhetskulturen kan påverka anställdas beteende. Kopplingen till säkerhetskultur och dagliga arbetet kan ses i det Alfawaz et al. (2010) skriver om att med hjälp av säkerhetskulturen blir ”göra rätt” en norm inom organisationen.

Det större delen av respondenterna nämner att förändringar kommer ligga i ökad medvetenhet kring vilka personuppgifter som behandlas och hur de behandlas. Per nämner att det kan leda till större försiktighet i hur känsliga personuppgifter hanteras, detta kopplar vi till att det är ett sätt för sjukvården att sätta sig och medarbetarna i bästa möjliga position för att skydda personuppgifter (Frye, 2007), samt kunna förstå och uppvisa rätt beteende i frågan (Wiles et al., 2012). Vidare styrkes vikten av medvetenhet i Katsikas (2000) slutsats om att alla medarbetare behöver medvetenhet och det McIlwraith (2016) skriver om att vägledning behövs för att bli medveten om det personliga ansvaret som medarbetare. Även Hassan et al. (2017) påpekar att säkerhetsmedvetenhet är en av de viktiga faktorerna som påverkar säkerhetskulturen. Vikten av de tre faktorerna, säkerhetsmedveten, säkerhetskunskap och säkerhetsbeteende, bör ha uppbackning av ledningen för att ha möjlighet att skapa en säkerhetskultur.

Respondenterna är inte helt överens om att det endast är systemen som behöver förändras som verksamhetsutvecklarna Per och Jenny främst förespråkar. Per och Jenny ser det som ett av de största problemen med implementeringen av GDPR i organisationen. Verksamhetsutvecklaren Karim och områdeschefen Karina trycker båda på hur de anser att utmaningarna för GDPR även kommer ligga i att ändra sättet som medarbetare arbetar och tänker kring personuppgifter och integritet. Precis som Malcolmson (2009) betonar att en säkerhetskultur kan påverka säkerheten i en organisation, därmed är det dels väldigt viktigt för sjukvården att se till att säkerhetskulturen finns implementerad i rutiner men det visar också på svårigheten att implementera en säkerhetskultur som kan stödja arbetet kring GDPR inom sjukvården. Alfawaz et al. (2010) betonar vikten av att skapa ett ramverk runt säkerhetskulturen och det är något vi uppfattar att man vill åstadkomma på de avdelningar vi har studerat.

5.3.1 Värdegrund

Kanslichefen Olivia och områdeschefen Karina talar mycket om att GDPR måste läggas in i det värdegrundsarbetet som finns inom Region Skåne. Karina anser precis som Ghazvini och Shukur (2017) och AlHogail (2015), att ha rätt resurser och lyfta ämnen kring personlig integritet och verkligen försöka få personalen att tänka till och förstå vad och hur personuppgifter behandlas inom avdelningen, är ett steg på väg till att implementera GDPR i arbetsplatsens kultur. Här menar Karina att hennes avdelningar är en bit på vägen genom att ha lyft och belyst GDPR för medarbetare, vilket AlHogail (2015) menar på kan leda till att organisationen blir mer effektiv i hur informationssäkerhet hanteras. Karim och Karinas pratar om problemen med att de ser patienten snarare än personen och vikten av det. Karina nämner de stigmatiserade grupper hon arbetar med på de avdelningar hon är chef över, går i linje med vad Hassan och Ismail (2016) och Metalidou et al. (2014) säger kring medvetenheten. Hur medvetenheten bör vara inbäddad hos medarbetaren samt om hur medarbetare ska hantera arbetsuppgifter på ett ansvarsfullt sätt utifrån ett informationssäkerhetsmedvetenhetsperspektiv. Detta ligger i linje med hur Karina och Karim vill att de ska arbeta med GDPR inom deras organisationer och hur det behöver implementeras i organisationernas kultur respektive värdegrund.

Verksamhetsutvecklaren Karim tar upp en viktig aspekt med att han inte tror att utbildning och träning av personal är ett fullgott arbetssätt för att implementera GDPR inom hans organisation. Katsikas (2000) instämmer med detta, att träning behövs men att det krävs mer involvering av medarbetarna för att kunna säkerställa en acceptabel medvetenhetsnivå inom organisationen. Dock är det många forskare inom informationssäkerhetsmedvetenhet som anser att utbildning är en av de viktigaste byggstenarna som behövs för att medvetandegöra informationssäkerhet inom organisationen (Ghazvini & Shukur, 2017; Shoniregun et al., 2010; Wiles et al., 2012). Olivia tar upp att hon tror att eldsjälarna kommer behöva hjälpa till att driva frågan och kan genom att lyfta frågan samt föra diskussion, hålla GDPR på en medveten nivå hos de anställda.

Dock kan vi inte riktigt se att någon av respondenternas svar överensstämmer med det som Hayden (2017) beskriver angående att uppmuntra till informationssäkerhet på samma sätt som medarbetarna motiveras till att arbeta patientsäkert och ge kvalitativ vård. Däremot så pratar respondenterna om att detta är något som de vill uppnå, framförallt trycker Karina på att uppmuntran till att arbeta på ett mer informationssäkert sätt, som något som de eftersträvar på hennes avdelning.

6 Slutsats

Studien ämnade att svara på frågan:

- *Vilka utmaningar möter en organisation och dess anställda – utifrån ett medvetenhetsperspektiv – vid en stor policyförändring som berör informationssäkerhet?*

Utifrån vår studie, har vi sett att hälso- och sjukvården har stött på flertalet utmaningar när det gäller förberedelserna inför GDPR. De befintliga systemen är inte tillräckliga för att kunna utföra vardagliga uppgifter på ett GDPR-säkert sätt. En så pass stor policyförändring som GDPR är berör organisationer på mer än ett sätt. Det som blev utmärkande var just bristen på förståelse inom organisationerna för vad policyförändringarna kommer innebära, samt viljan i organisationerna att förbättra denna medvetenhet genom att implementera kraven för GDPR i organisationskulturen.

Alla deltagare i studien var rörande överens om att medvetenhet krävs för att kunna implementera en så pass stor policyförändring. Många ansåg dessutom att nyckeln till att lyckas implementera policyförändringen ligger i ett värdegrundsarbete och i organisationskulturen inom verksamheten. Detta på ett sätt som gör att de arbetsuppgifter som påverkas följer policyns riktlinjer och därmed också följer lagen. På så vis kommer säkerhetskulturen att påverkas inom organisationen.

Vi ser att de utbildningar som finns i organisationerna inte har varit nog för att skapa den medvetenhetsnivå som krävs för att kunna följa riktlinjerna för en policyförändring, såsom GDPR. Utbildningar som idag rör exempelvis hantering av personuppgifter är inte nog för att följa GDPR. Detta gör att vi anser att en så pass stor policyförändring, som kommer påverka hela verksamheten på ett eller annat sätt, behöver både ha stödjande system för att förändringen ska uppfylla eventuella lagkrav och skapa en medvetenhet kring hur de ska användas. Vi ser därmed en utmaning i att policyförändringen kommer behöva medvetandegöras genom att implementeras i organisationskulturen, och i arbetet med de värderingar som uppmuntras av policyförändringen.

Vi ser också att det är av yttersta vikt att en policyförändring som rör informationssäkerhet och påverkar hur dagliga arbetsuppgifter utförs, ingår i den säkerhetspolicy som företagen har. Detta är för att kunna säkerställa att den nya policyn följs och för att upprätthålla en utbredd medvetenhet kring informationssäkerheten i en organisation, vilket annars kan komma att bli en utmaning för organisationer.

Sammanfattningsvis ser vi att det blir viktigt att implementera en policyförändring som rör informationssäkerheten i en säkerhetspolicy. Detta för att säkerställa en viss medvetenhetsnivå hos de anställda. Vidare ser vi att medvetenheten kring informationssäkerhet inte är tillräcklig för att kunna utföra de vardagliga arbetsuppgifterna på ett informationssäkert sätt. Detta kan i sig leda till att ett felaktigt beteende blir accepterat och kan därmed utgöra en säkerhetsrisk. Till sist ser vi även att säkerhetskulturen bör prioriteras för att kunna skapa medvetenhet i en organisation där policyförändringen påverkar dagliga rutiner. Vi upplever inte att det endast räcker med utbildning och information kring informationssäkerhet, utan att det krävs en djupare förståelse för att kunna utföra arbetsuppgifter på ett korrekt sätt. Därför behöver organisations- och säkerhetskulturen involveras.

6.1 Vidare forskning

Då denna studien har ett litet omfång anser vi att vidare forskning kan behövas för att följa upp om varför inte utbildning är tillräckligt för att medvetandegöra informations säkerhet. Samt hur säkerhetskulturen påverkar informations säkerhetsmedvetenheten inom organisationen. Detta bör förslagsvis göras med fler respondenter och på flera olika organisationer med en större geografisk spridning.

Appendix 1 – Intervjuguide

Din roll

- Berätta lite om dig själv och din roll på din arbetsplats?

GDPR

- Hur har förberedelserna inför GDPR sett ut?
- Hur har GDPR påverkat dig och dina arbetsuppgifter?
- Vad krävs i en organisation för att GDPR ska följas?
- Vad blir den största förändringen i den dagliga verksamheten, i och med GDPR?
 - o Vem berör den nya lagstiftningen?
 - o På vilket sätt?
- Vilka utmaningar finns inom organisationen inom GDPR?
- Har det skett en sådan här större förändring förut? (informationsrelaterad - säkerhetsrelaterad)?
 - o Kan du ge ett exempel?
- Hur hanterades denna?
- Vilka problem uppstod?

Awareness

- Hur går man tillväga för att informera om GDPR? - Utbildning, föreläsningar, praktisk träning?
- Vilket upplägg har man på utbildningar?
- Är informationen om GDPR en kontinuerlig process eller ges den en gång?
 - o Om kontinuerlig, hur är det tänkt att utformas?
- Anser ni/du att det är viktigt att medvetandegöra GDPR för personal?
 - o Varför/varför inte?
- Hur gör man för att medvetandegöra?
- Vad tänker sig organisation att de vill uppnå med att medvetandegöra?
- Har ni fått någon respons från personal på eventuella förändringar i den dagliga verksamheten eller överlag?
 - o Har ni mött något motstånd/hur har det mottagits?
- Finns det en standard för medvetandegörande av stora policyförändringar såsom GDPR?
 - o Anpassas dessa i så fall till situationen eller är de alltid likadana?
- Jobbas det med informationssäkerhets medvetenhet i det dagliga arbetet?
 - o På vilket sätt? Varför inte?
 - o I så fall, hur gick man tillväga?
- Har du varit involverad i något annat program som har haft med medvetandegörande av informationssäkerhet?

Avslutning

- Anser du/ni att vi har missat att fråga om något? Är det något du/ni vill lägga till?

Appendix 2 – Intervju 1

Organisation: SUS, Skånes Universitetssjukvård

Intervjuperson: Olivia Hjorth

Yrkesroll: Kanslichef

Tid och plats: 11.00-12.00, tisdagen den 10 april 2018, personligt möte i Lund

I: Intervjuare

O: Olivia

Referens	Respondent	Frågor och svar
IP1.1	I:	Då kan vi börja med det, din roll om du vill berätta lite om dig själv och din roll?
IP1.2	O:	Ja, jag är då kanslichef här på SUS och i förhållande till GDPR då så är jag projektledare för GDPR. Och varför jag gör det är för att kansli har ansvaret för PUL-registret, registret för personuppgiftsregistreringarna då. Det har legat som ansvar på kansliet. Så när jag började här då, vid årsskiftet så behövdes det någon som projekt-ledde det här arbetet. Så jag är projektledare för GDPR och kanslichef till vardags.
IP1.3	I:	Nu då inför GDPR, hur har förberedelserna sett ut?
IP1.4	O:	Ja, det finns ju ett stort övergripande projekt i Region Skåne som är det övergripande projektdirektivet. I juni i fjol så fick vi ett uppdrag av regiondirektören, som gick ut i alla förvaltningar då för förberedelser för GDPR för att ta fram en projektplan, övergripande. Sen har man då utsett ansvariga på SUS för att driva det här arbetet. Nu var det ju så att SUS genomgick en stor omorganisation i princip samtidigt då vid ju och till årsskiftet, vilket gjorde att då det inte blev jättemycket framdrift i GDPR-projektet här. Det projekt-team som startades upp under hösten är det faktiskt bara en person kvar i dagsläget. Men grundläggande är ju att vi har försökt följa dem projektdirektiv som har kommit vilket har varit inledningsvis inventera alla personuppgiftsregister som vi har i sjukvården men också att städa, det vill säga att alla medarbetare ska gå igenom sina personliga mappar och sin epost för att kolla. Vi har ju väldigt många medarbetare här som arbetar hela tiden med personuppgifter i och med patienter och vi har ju väldigt mycket forskare som använder sig av patientuppgifter i sin forskning. Så det har varit väldigt nyttigt och har lyft på locket på en jättestor frågeställning som handlar om arkivering och radering som en del av städarbetet för GDPR. Inventeringsmässigt så har, vi är ju en väldigt stor organisation, vi har ju 14 000 anställda så vi har på varje verksamhetsområde en kontaktperson som vi kommunicerar framförallt med och sedan har de i sin tur en kontaktperson på varje enhet som de kommunicerar med. De här kontaktpersonerna ansvarar för att driva frågan internt i deras område. Det är ju alltid enhetschefen och verksamhetschefen som ser till att arbetet görs, de har lite mer kompetens. Så vi har genomfört fyra utbildningstillfällen för kontaktpersonerna så att de ska ha lite mer på fötterna. Sen finns det ju då lite utbildningsmaterial som egentligen är gemensamt för hela Region Skåne som de här kontaktpersonerna använder sig utav sen har vi en funktionsbrevlåda där de skickar sina frågor framförallt. Som vi försöker besvara så fort vi kan, det är inte alltid vi har kompetensen själva, vi använder ju oss också av det regionala projektteamet. Där vi har avstämningar en gång i veckan, där vi kan ta upp frågor som vi inte kan lyckas svara på själv, och det är ju tydligt att det inte är alla frågor som är kristallklara. Och eftersom vi nu fokuserar på att inventera så gör vi det genom att bara titta på "vad finns det idag?". Vi gör alltså inte arbetet som handlar om att säkerställa att det är korrekt. Förvaringsplatser till exempel hanteras korrekt, utan just nu försöker vi bara inventera "Vad finns det?" och denna och nästa vecka så pågår det en analys av det resultat som kommit in. Det är inte alls komplett, vi är ju en jättestor organisation, vi vet inte ens hur mycket vi borde få in i slutändan. Men vi har fått in ungefär 300 olika platser som

		man förvara register. Så nu håller vi på att analysera frågeställningar: hur många av dessa ligger på ett korrekt ställe och skyddat sätt och vad kommer vi behöva göra utöver de redan kända problemen vi har. För att vi ska kunna leva upp till GDPR kraven.
IP1.5	I:	Just det här med GDPR, hur har det påverkat dig och dina arbetsuppgifter?
IP1.6	O:	Jag har ju inget före GDPR om man kan säga. Utan vad det har gjort och som jag tycker är väldigt positivt är att det har satt ljuset på arbetsuppgifter som finns inom kansliet på ett sätt som var välbehövligt. Det har väckt frågan kring arkivering och gallring som ligger i kanslifunktionen. Vilket gör att vi nu har en möjlighet att hoppa vidare med de frågorna, från att det tidigare har varit lite styvmodigt behandlat område. Mer än så här: Jaja vi vet arkivering, ungefär så. Tills att man nu: vad gäller verkligen, gör jag rätt. Det är ju en väldigt bra öppning, vi lägger ju väldigt mycket tid på den typen av frågor just nu från att det kanske varit en liten procent varje vecka, så lägger vi 20–30 procent hela kansliet på detta just nu på denna typen av frågor.
IP1.7	I:	På vilket sätt tycker du att det har varit en positiv förändring i det dela?
IP1.8	O:	För min del så ger det då en möjlighet att faktiskt driva den här typen av frågor på ett annat sätt med en annan kraft. För att vad GDPR gör är att sätta ljuset på den svaghet som finns i organisationen, kring kompetensen, kring de här frågorna, hur vi faktiskt gör och i och med att folk nu har entydig medvetenhet, brist i kompetens och brist i medvetenhet får en väldigt tydlig påverkan på organisationen om man skulle börja granska oss med GDPR glasögon. Vilket ju kan komma att hända, det vet vi ju inte hur man kommer att tillämpa lagstiftningen när den väl är på plats. Men det gör då att vi kan använda oss av den medvetenheten och börja jobba mer strukturerat och... Tidigare har vi försökt trycka ut informationen, men nu drar man informationen till sig och vi ska bara försöka använda oss av den kraften så att vi står bättre rustade för den här typen av förändringar framöver.
IP1.9	I:	Vad tycker du då krävs i en organisation för att GDPR ska följas?
IP1.10	O:	Omg, nä men tillbaka lite till det här, det är ju lite olika delar, om man verkligen zoomar ut och pratar om vad som ligger bakom GDPR så handlar det ju egentligen om vår förmåga att sköta vårt myndighetsuppdrag på ett korrekt sätt så att vi kan stå för varför vi använder uppgifterna, varför vi behöver ha in dem och att egentligen är samhället uppbyggt på tillit på att vi hanterar och använder oss av uppgifter på ett sätt som är korrekt och säkert för våra medborgare. Den vetenskapen behöver man ju ha i ryggraden hela tiden, det som upplevs som en besvärande pålaga har ett gott syfte. Det är mer en sådan övergripande medvetenhet som borde finnas. Sen behöver det finnas en god vilja att känna till de krav som ställs på arkivering och gallring, hur skapar man det: jo genom att det finns bra system som underlättar och att man har arbetat med frågorna så att gamla rutiner som man har jobbat in att man ständigt förnyar dessa så att man inte ligger kvar i det gamla sättet för att det var så vi behövde göra med system X men nu har vi system Y, då måste vi jobba med systemet för att förenkla arbetssätten och säkerställa att det flyter på smidigt och tyvärr är det så att man tar arbetsätten från det föregående systemet och försöker lägga det ovanpå det nya så resulterar det i att man gör en extra kringelkrok. För att man är van vid att göra det eller tror att det krävs eller så. Det behövs ju en förnyelsetanke kring det också så att man har ögonen på vad är det som behöver förbättras och det är ju också en attitydfråga, men sedan är det ju självklart att systemen ska stötta i det här, behöver ju vara bra och där har vi ju en jätteutmaning i GDPR. Det att vi har ett så otroligt stort antal olika IT-system men personuppgifter i sjukhusvärlden men också att de här system är ju byggda i, en väldigt stor utsträckning, i en tid när de här kraven inte har funnit och det finns väldigt många egenutvecklade applikationer i sjukvården som gör att de som har byggt dem, aldrig har haft den här tanken med att man ska kunna söka ut uppgifter, och extrahera dem om någon efterlyser det, därför finns inte de funktionerna. Det är ju en utmaning i en organisation för att det här ska fungera så bör det finnas rätt mängd medvetenhet om syftet och ständigt förbättringstanke men också bra system som stöttar i arbetet.

IP1.11	I:	Om man ser då på förändringar, i den dagliga verksamheten, vad blir den största förändringen i och med GDPR?
IP1.12	O:	Min förhoppning är väl egentligen såhär att när dammet har lagt sig så ska ju inte de behöva ha några stora förändringar i sitt arbete dagligdags. Utan vad som ska ha hänt är väl snarare att de lägger filerna på en säker plats som då ska finnas och att man helt enkelt jobbar in den medvetenheten om personuppgifterna kopplat till säker lagring så att det är ju ingen jättestor förändring i, mer att man riktar arbetssättet lite annorlunda. Istället för att spara på en öppen G mapp så sparar man på en säker plats. Eller att man kanske mer regelbundet städar upp efter sig i sina mappar men det är ju kanske inte det dagliga utan mer att man rutinmässigt säkerställer att man slänger filer som man inte längre behöver.
IP1.13	I:	I och med detta, att slänga och rensa, vem berör den nya lagstiftningen och på vilket sätt?
IP1.14	O:	Hos oss är det ju väldigt många som blir berörda, men det är ju bara naturen av jobbet här att man jobbar med patientuppgifter. Framförallt så är det ju sekreterarna som handhar olika former av register och uppställningar, en del har det för sin egen skull som mottagningar och liknande och andra har ju det för forskning och då är det ju läkare och administrativ personal som stöttar läkarna och sjuksköterskor som forskar eller om man har hand om andra specifika arbetsuppgifter. [exempel] Det finns ju allt möjligt man kan behöva ha register för avlidna och det är ju dom som administrerar och handhar det. I princip så blir det ju väldigt brett och det är ju inge yrkesgrupp som man specifikt, förutom forskarna, generellt alla forskarna. Men annars är det olika personer i de olika avdelningarna beroende på vad de har. Vi har ju all annan administrativ personal som jobbar, då handlar det ju inte så jättemycket om patientinformation utan då handlar det mer om personal och det administrativa och det ska ju också handhas på ett korrekt sätt, men inte med samma implikationer som med patienter. Var det svar på frågan?
IP1.15	I:	När du säger register, jag har ju själv jobbat inom sjukvården, hur påverkar det de här centrala registerna som man säger exempelvis inom hjärtsjukvården, där de registrerar hjärtpatienter då?
IP1.16	O:	ja allt sådant måste ju finnas. Man måste ju göra den här bedömningen, har vi laglig grund för att ha det? Förvarar vi det på ett korrekt sätt? Har vi bara de uppgifterna i dem som faktiskt krävs för arbetet och inga extra uppgifter? Hur hanterar vi det? Och vem tar ansvar för det? Hur hanteras det när vi till exempel är färdiga och vad är planen med det? Är det ett sådant register så ska det ju vara registrerat i vår PUL-översikt på ett korrekt sätt och vara etikprövat oftast då också. Det berör dem absolut och det är därför som vi upptäcker att det är en hel del som ligger och flyter. Folk har lämnat organisationen, eller i vårt register så står det att det är en person som är ansvarig som kontaktperson. Vi skickade ju ut mejl till alla som stod som kontaktpersoner för de olika förteckningarna i PUL-registret, där har vi över 500 aktiva register. Då blev det ju väldigt tydligt det här, det står en person som är inskriven som kontaktperson för 10-12 år sedan för att det har varit en lång studie, som sedan står som frågetecken [kontaktpersonen] på hur de fortfarande kan stå kvar som kontaktperson. Ibland har vi ju upptäckt att vi har dubbla registreringar för att någon har registrerat det för 12 år sedan och så för 6 år sedan så gjorde någon en ny registrering som man kan uppfatta är till samma register, för etikprövningen är ju densamma. Men man har inte känt till den första registreringen och därför registrerat om den. Så vi hittar ju mycket sådana saker just nu när man sätter ljuset på det. Så det påverkar ju verksamheten starkt just nu då det skapar väldigt mycket stress. Jag hade en diskussion med hjärtmedicin, där vi har fått mejl om några register som vi inte ens vet var register finns rent fysiskt, alltså var i våra datasystem, där det står att verksamhetschefen är ansvarig men registerna i sig vet vi inte vem som har varit från början och var det finns. Så att alla sådana frågor sätts ju på sin spets och det skapar ju nervositet och stress. Man vill ju göra rätt, det är ju ändå den grundförutsättningen, att man vill göra rätt.
IP1.17	I:	vilka utmaningar ser du att det finns i organisationen i och med GDPR?

IP1.18	O:	vi har ju i dagsläget egentligen inte tillräckligt bra IT-system, vi har inte tillräckligt säkra lagringsplatser med tillräckligt effektiv behörighetskontroll. Vi saknar utbredd kompetens på arkivering och gallring framförallt. Och vi har inte idag en organisation som är anpassad för de krav på registerutdrag som kommer komma i och med GDPR. Redan idag med ett registerutdrag per person och per år så har vi ibland svårt att få igenom det i en rimlig tid. Och med det nya kravet på att man ska kunna göra det flera gånger om året till samma person, plus den uppmärksamhet som GDPR fått i samhället så är jag rädd att vi kommer ha en räl utmaning i att hitta rutiner och fungerande arbetssätt för att kunna leverera alla de registerutdragen. Så rent praktiskt.
IP1.19	I:	just det här med förändringar i GDPR, har det varit någonting tidigare, en större förändring.
IP1.20	O:	När PUL kom 98 antar jag, men jag vet faktiskt inte. Jag har bara varit här på SUS i 6 år och kan inte komma ihåg att vi har gjort någon sådan stor förändring under den perioden, så genomgripande. Men det har vi säkert.
IP1.21	I:	Det är ingen som har med informationssäkerhet att göra som du känner till?
IP1.22	O:	Säkerligen, men inget som jag kan komma på eller känner till. Jag vet inte när man har ändrat till exempel patientdatalagen eller i dataskyddslagen eller så som har påverkat oss. Då får ni prata med info.sek.
IP1.23	I:	Hur går man tillväga inom SUS då för att informera om GDPR?
IP1.24	O:	Framförallt så har vi ju då försökt nå ut via dem här kontaktpersonerna. Vi har ju så klart varit ute och informerat på förvaltningsledningsgruppen och dom i sin tur tar ju vidare det till sina ledningsgrupper, men huvudsakligen är det via kontaktpersonerna. Sen så skickar vi ju ut informationsmaterial eller små artiklar via våra interna kommunikationskanaler som intranätet, chefsnytt och sus-nytt. Vi har såna här stormöten som kallas ledningens månadmöte där man informerar, där vi varit och pratat om det. Vi hade i förra veckan ett väldigt välbesökt seminarium riktat till forskarna kring GDPR. Vi har sett ett speciellt behov där och där har vi filmat hela det seminariet så det kommer ligga ute också. Så att liksom bit för bit försöker vi ju att sprida medvetenheten om GDPR. Jag upplever att den är ganska god, kontaktpersonerna tar ju kontakt med alla sina kollegor på enheter och så vidare. Men vi har ju de facto ingen, det finns ju ingen statistisk räkning så jag vet inte om vi har verkligen nått ut till alla 14 000. Vi ser ju materialmässigt, så ser vi ju att vi inte fått in tillräckligt för att täcka det faktum att alla våra 14 000 medarbetare skulle vara ordentligt inventerade. Men min uppfattning är ändå att medvetenheten är ganska hög, för det är stor aktivitet och det kommer många frågor.
IP1.25	I:	Förutom föreläsningar då att man pratar om det, finns där någon form av utbildning som genomförs?
IP1.26	O:	Nej, vi har ingen utbildning just nu. vi väntar faktiskt på SKL kommer med en generell GDPR utbildning som Region Skåne tänker att vi ska använda oss av för nyanställda till exempel och till de gamla anställda också för den delen framöver. Så vi kommer väl att jobba med den, jag har ingen aning om hur lång eller vad SKL tänker sig baka in i den, det kommer man inte veta förrän den kommer.
IP1.27	I:	Om man då ser just informationen om GDPR, kommer man inom SUS se det som en kontinuerlig process där man försöker medvetandegöra det under hela tiden eller är det bara att man får informationen en gång och sen ska man kunna det?
IP1.28	O:	Lite det som jag sa inledningsvis, jag ser ju det här som en möjlighet att egentligen att göra ett framåttryck som handlar mer allmänt om hur vi hanterar information och hela arkiverings och gallrings biten är förknippad med detta. Registerutdrag och sånt som kommer landa på mig eller snarare kansliheten menar jag, kommer vara beroende av att man känner till och att man är medveten om de här frågorna. Målsättningen är ju att vi ska ha en fungerande organisation kring

		de här frågorna, då menar inte jag att det ska finnas personer som är anställda specifikt för detta, utan mer att det ska finnas väldigt tydliga uppdrag och ansvar ute i verksamhetsområdena för att de här frågorna kan hanteras ner på enhetsnivå där de behöver finnas. Och det arbetet håller man ju på med nu parallellt här, med att identifiera hur ska detta se ut och vad är det för typ av uppdrag som behöver kännas till och vilken kompetens kommer behöva finnas ute på verksamhetsområdena för att man ska kunna genomföra det, vilka typer av rutiner, hur ska vi liksom bygga upp det här. Så att nej det är ju absolut inte någon, så funkar inte lagstiftning, nu är det ett projekt som handlar om att göra organisationen redo för att svara mot GDPR, men framöver så kommer det ju handla om att vi ska fortsätta upprätthålla och förnya/förbättra vårt myndighetsansvar i de här frågorna.
IP1.29	I:	Och just det här med medvetandegörande, anser du då att det är viktigt att medvetandegöra just GDPR för de anställda?
IP1.30	O:	Ja, alltså GDPR har blivit liksom, det har blivit en slogan. Det medvetandegör det här att det är en del av vårt uppdrag, att visa på att vi tar ansvar för dels för vår roll som myndighet men också att de personuppgifter som finns hos oss är trygga och att vi faktiskt kan berätta varför vi har de personuppgifter vi har och vad vi gör med dem. Det har vi alltid egentligen behövt kunna redogöra för, men GDPR sätter ju som sagt ljuset på och det blir en mycket starkare/skarpare lagstiftning som gör att det man tidigare kanske har kunnat sopa in i hörnet lite behöver dras fram nu i ljuset och verkligen säkerställa att vi förstår varför vi gör det. Sen är ju det här som allting annat, det här handlar om den infrastruktur på vilken vi har vårt myndighetsutövande och samhällsgrunden hos oss, det här att vi förlitar oss på att vi har stora institutioner som kan vara så pass stadiga, stor och transparenta så vi känner tillit till dem. Och det, jag tror vi kommer ha en utmaning framöver att faktiskt leva upp till det och där är jag inte säker på att alla är medvetna om det idag, men jag tror att medborgaren är mer medveten om det kravet. Och det gör ju också igen att det behöver byggas in lite grann i ryggraden på något sätt, kanske inte att det alltid ligger längst fram i pannan men det är liksom lite grann som det här att vi gör allt för patienten så behöver vi också bygga in det här. Vår organisation finns för medborgaren och det myndighetsansvar som finns med det, Hur man nu ska göra det, jag vet inte, Matrix.
IP1.31	I:	Det här med att medvetandegöra hur gör man då, för de anställda för att liksom få in det i ryggraden?
IP1.32	O:	Ja, alltså om man säger förändringskommunikation om du ska medvetandegöra nånting eller nånting ska fastna och sånt, så säger man att det måste repeteras minst sju gånger. Och eftersom vi vill att det här ska vara nånting kontinuerligt levande arbete så betyder det också att vi behöver hitta ett sätt att arbeta med frågan som blir en naturlig del av vardagen. Och det är alltid en jättestor utmaning i en så här stor organisation, men man kan komma dithän då genom det här, dels att det är en naturlig del av introduktionen. Det är klart att vi måste ta hand om all personal som redan finns här, men jag tror verkligen på att man måste vara noggsam med att föra in det som en naturlig del när man kommer, att det här är en del du möter, du får med dig det. också att man fortsätter att stötta de eldsjälar som finns ute i verksamheterna som lätt tar till sig det här och känner att det här är viktigt och vill driva dem här frågorna eller står för dem här frågorna. Vi har olika nätverk ute i organisationen som jobbar till exempel med arkiv då och dem behöver man ju fortsätta hjälpa och stötta för att ta till sig dem här frågorna, så dem kan vara experter för sina respektive enheter. Men sen måste man också hjälpa enhetschefer och verksamhetschefer att känna att det är lätt att ta ansvar i dem här frågorna. Jag ser det som en ganska långsiktig process, det är inte så att jag tror att jag i slutet av året kommer ha omvänt hela organisationen till att GDPR är en naturlig del av deras vardag. Men jag tror att vi kommer ha tillräckligt många för att de arbetet ska kunna fortsätta genomsyra det som nästan vilket värdegrundsarbete som helst, det är långt och traggligt och man behöver hålla fokus under väldigt lång tid och när man inte behöver hålla fokus längre är när fokus finns naturligt.
IP1.33	I:	Vad tänker sig SUS då att ni vill uppnå just med det här att medvetandegöra GDPR?

IP1.34	O:	Att vi ska kunna leva upp till det myndighetsansvar vi har, att vi ska kunna vara en samhällsinstitution som faktiskt lever upp till dom krav som, lagstiftningen är ju egentligen en reflektion av dom krav som samhällsmedborgarna ställer. Och där vill vi ju faktiskt att vi ska vara duktiga, inte bara duktiga men att det ska vara så pass naturligt att det inte ens är något vi medvetet känner att vi måste traggla på utan det bara funkar. Så det är ju egentligen den långsiktiga målsättningen är ju att det är lika naturligt som det är att andas och att vi sköter vår data.
IP1.35	I:	Och har ni då fått någon respons från dem anställda på eventuella förändringar i den dagliga verksamheten eller överlag inom SUS?
IP1.36	O:	Nej, i dagsläget så handlar det om , många vill ju gärna hoppa till hur ska jag då göra och som det är nu under inventeringsfasen så blir det ofta : just nu så behöver du inte göra någonting annat än att tala om för oss att dem här filerna existerar och att dem behöver ha en inramning eller du behöver tänka annorlunda. Beskrev innan lite den här nervositeten att man vill göra rätt och den är mest påtaglig just nu och att man verkligen frågar hur kan jag göra rätt, jag ser i det här idag att jag inte gör rätt hur kan jag göra rätt. Och det är inte alltid vi kan svara på rak arm och ofta kan det handla om IT-systemen, att dem inte är korrekt konfigurerade för det här. Men inte så här att någon har diskuterat hur dom kommer vara tvungna att göra i sitt verkligt praktiska arbete annorlunda varje dag, dom frågorna tar dom inte med oss.
IP1.37	I:	Har du märkt att det finns något motstånd mot just förändringarna och medvetandegörandet av GDPR?
IP1.38	O:	Nej, jag skulle inte vilja påstå att det är något motstånd men det finns dem som tror att personuppgiftsombudet skapat reglema/lagen och därför vänder sig dit med frågan hur har du tänkt nu. Och det är mer grejer som man kan bli full i skratt av över att man tänker att lagstiftningen är något vi sköter lokalt på SUS eller i Region Skåne överhuvudtaget, så är det ju inte. Jag upplever faktiskt inte så mycket motstånd, det är klart att folk blir frustrerade över tidsaspekten och det hade jag också varit, vi började inte i tid på SUS det började ganska sent. Men dom är inte motståndare till arbetet utan snarare är det, det här att det är så mycket vi måste göra. Sen tror jag också att det finns ett passivt motstånd eller snarare ett motstånd som är mer att man är passiv, att man inte kanske gör det man behöver göra, men dem märker vi inte så mycket av utan det kommer vi märka först när vi börjar räkna in alla verksamheter och kan börja se ok dom här verksamheterna har inte gjort, vi har inte en enda registrering från dem, vi har inte en enda inrapporterad fil från dem. Då kommer vi se att det finns oär där man kanske inte har gjort så mycket, men i dagsläget och kontaktpersonerna ute är väldigt aktiva. Ur det perspektivet så upplever vi snarare det här: vill göra rätt, frustrerade över att det inte är enkelt, frustrerade över tolkningar, de kan vara frustrerade över våra IT-system, men inte att man har motstånd mot själva arbetet som sådant.
IP1.39	I:	Inom SUS/Region Skåne finns det någon standard för hur man medvetandegör en stor policyförändring liknande GDPR?
IP1.40	O:	Nej, det finns inte.
IP1.41	I:	Om man då tittar just på information och informationssäkerhet, jobbas det just med informationssäkerhets medvetenhet i det dagliga arbetet?
IP1.42	O:	Det upplever jag inte att det gör. Det finns en utbildning men det blir ganska tydligt att den är okänd.
IP1.43	I:	Har man på något sätt, just den här utbildningen som du nämner, är det på något sätt man gör för att få fler att gå den/ta del av den?
IP1.44	O:	Nej, då är vi inne på Info.sek, nej jag tror inte, inte annat att den ligger med som en del av utbildningarna man ska gå när man introduceras. Vi har inte gjort någon push nu för den utbildningen eller snarare så här, när det blivit mycket frågor kring arkiv och gallring har vi hänvisat till vissa utbildningar. Men vi har inte

		gjort någon större utbildningsdrive. Det är alltid en avvägning i såna här lägen, vad ska vi lägga tid på och eftersom det krävs väldigt mycket tid på det faktiska inventerandet så har vi inte pushat för utbildningsinsatser i dagsläget. Och som sagt GDPR utbildning kommer sen och där kommer man behöva titta på en prioriteringsordning på hur man ska säkerställa vilka, var, när och hur man ska gå den, hur akut är det att man går den initialt, för vilka grupper är det helt centralt att man går den. Jag tänker till exempel medicinska sekreterare, det måste vara en del av deras grundutbildning när de kommer hit även om de nyutbildade har det med sig in, men är man lite äldre och nyanställd så har man kanske inte stött på det. Alltså det är alltid en avvägning och oaktat att det handlar om tid så är tid alltid lika med en kostnad för verksamheten och speciellt i dagsläget är vi ständigt underbemannade på alla positioner, så då får man också göra en prioritering som säger att vissa grupper kommer ha en utbildning initialt och andra lite senare.
IP1.45	I:	Har du på något sätt varit involverad i något annat program som haft att göra med medvetandegörande av informationssäkerhet?
IP1.46	O:	Inte i medvetandegörande i informationssäkerhet. Det här är inte min bakgrund. Jag har jobbat mycket med förändringsarbete men inte just inom informationssäkerhetsområdet.
IP1.47	I:	Är det något vi missat fråga dig om som du tycker vi borde ha med oss?
IP1.48	O:	Nej, det ganska heltäckande det ni presenterat, jag kan inte komma på någonting.
IP1.49	I:	Du sa att man inte hade tillräckligt med kompetens, hur anser du att man behövt göra för att skaffa sig den kompetensen?
IP1.50	O:	Det är inte individen som sådan alltid som ska läggas till last där, utan det jag tänker är att vi inte alltid haft ett systematiskt sätt att introducera och underhålla den kompetensen ute i organisationen. Det är klart att man alltid som individ har ett ansvar för att ta reda på saker, men om det inte medvetandegörs att en fråga är viktig, så kan det bli att den hamnar längst ner i prioritet. Det som vi behöver göra framöver handlar om att säkerställa att alla som är nyanställda får en bra introduktion i exempelvis arkivering och gallring som en del, men också att dem som har ansvaret för den här frågan ute på enheter har tillräckligt med mandat för att prata om det och också är välkända inom sina egna organisationer, så folk vet vart dem ska vända sig. Och att dem kontaktpersonerna knyts ihop på ett sätt som gör att dem känner en trygghet i en grupp för att iom det är baserat på den här lösa nätverksstrukturen så krävs det att det finns ett tydligt ansvar och att enhetschefen får ett tydligt ansvar för de här frågeställningarna. Att det finns både en utförarorganisation och en ansvarsorganisation som liksom hänger samman. För då får dem här frågorna fokus och det blir automatiskt/lättare för den här typen av frågor att få plats i organisationen och därmed att kompetensen blir prioriterad.
IP1.51	I:	Vi tackar för intervjun och överlämnar en liten gåva som tack för deltagande.

Appendix 3 – Intervju 2

Organisation: Unilabs, Radiologi Sverige

Intervjuperson: Karim Ben Fredj

Yrkesroll: Verksamhetsutvecklare

Tid och plats: 10.00-11.00, fredagen den 13 april 2018, Skypemöte i Lund

I: Intervjuare

K: Karim

Referens	Respondent	Frågor och svar
IP2.1	I:	Vill du berätta lite om dig själv och din roll på Unilabs?
IP2.2	K:	Karim heter jag och är verksamhetsutvecklare Radiologin i Sverige, Jag har tidigare verksamhetschef och driftchef och från början röntgensjuksköterska med magister i medicin. Jag har jobbat i Unilabs i fyra år och ansvarar för utvecklingen generellt.
IP2.3	I:	Hur har förberedelserna för er sett ut inför GDPR?
IP2.4	K:	Efter egentligen en längre process, var man ska lägga ansvaret inom företaget för GDPR introduktionen. Så beslutades att det skulle vara i Group? Vilket innebär att vi är en stor koncern för som Unilabs är. Och då skulle det inte läggas på den nationella nivån. Då har man gjort en utredning om vem man skulle gå med då blir det Bird & Bird, en advokatfirma baserat i Frankrike. I november så inkluderande man också nationerna i detta. Då var vi nere i Paris och träffades på en kickoff och nu följer vi då en plan i samarbete med Bird & Bird.
IP2.5	I:	Om man tittar då på organisationen, Vad krävs det för att GDPR ska följas?
IP2.6	K:	Vi håller på faktiskt att göra en GDPR organisation. Men den GDPR-officer och så vidare, men nationsansvariga. Men det kommer bli en egen organisation i organisationen. Som besvarar GDPR frågor och sedan självfallet så kommer ju det också vara en del av ens vardag för att förstå detta ju.
IP2.7	I:	På vilket sätt blir det en vardag då?
IP2.8	K:	Vardagen med GDPR bli ju även som vi bygger en organisation i organisationen som kommer ta hand om de huvudsakliga övergripande frågorna så är det ju också viktigt att varje medarbetare i slutändan förstår innebörden av GDPR och framförallt som medborgare också, så i slutändan så kommer ju också alla påverkas av GDPR och de frågor som kommer uppstå kommer ju inte bara var riktade till organisationen som driver GDPR utan det kommer ju i första hand att vara till våra medarbetare.
IP2.9	I:	Om man tittar på förändringar i den vanliga verksamheten i och med GDPR vad blir den största förändringen?
IP2.10	K:	Det beror på vilken del av organisationen vi tittar på. Om jag tänker på patientflödet som är vår core-business ändå, vår huvudsakliga business, så blir det för patienten ingen större påverkan än att man möjligtvis måste fylla i något samtycke i vissa avseenden eller när det gäller vissa studier och så vidare men vi följer ju patientlagen och utifrån den så tror jag inte att det kommer påverka det dagliga för det så mycket. Det är snarare förståelsen av informationen. Om man tittar exempelvis på när undersökningen är gjord. Att vi i nuläget kanske sekretess, anonymiserar bilderna när vi skickar vidare bilderna kanske inte blir tillräckligt. Att ha större kunskap om vad ägandet är av försändelsen och framförallt att

		upprätta biträdesavtal mellan leverantörer och oss. Så vi tydliggör var ansvaret ligger.
IP2.11	I:	Om man då tittar inom organisationen, vem berör den nya lagstiftningen? Och på vilket sätt?
IP2.12	K:	GDPR berör väl alla? Sen är det förståelsen av GDPR, hur den ska användas. Jag tror inte i det vardagliga arbetet eller som medborgare eller som arbetstagarare eller som patient så berörs väl egentligen inte nämnvärt. Snarare när någonting inte fungerar, när auktoriserar man GDPR kortet. Den kommer ju inte vara överordnad hälso-och sjukvårdslagen exempelvis. Vi kommer ändå ha de förhållningsreglerna, vi kommer ändå spara bilderna i tio år även fast en patient kommer att säga att jag vill att ni raderar mina bilder. En medarbetare kan inte begära att vi kan radera dess uppgifter när anställningen upphör för då har vi andra lagar att förhålla oss till. Som svar på din fråga så berör den ju alla på olika sätt. Men det är förståelsen av den som kommer svåra den stora utmaningen.
IP2.13	I:	Hur tror du att den utmaningen på bästa sätt kan lösas?
IP2.14	K:	Bästa sätt kommer jag kunna svara på om tre år. [skrattar]
IP2.15	I:	Har du några indikationer på hur de kan lösas i och med era förberedelser?
IP2.16	K:	Ja, jag tror att varje persons ska förstå var avgränsningen till GDPR börjar och slutar. För jag tror i det fallet, om en patient kommer in och säger: Är ni GDPR kompatibla, mina bilder hur sparas dem? Då ska vi ändå kunna reflektera över att dina bilder sparas på samma sätt som de gjorde innan GDPR och vi tar fullständigt ansvar i Sverige utifrån de lagar och förordningar vi har. Att vi har en ökad förståelse för det. Medan andra länder kommer ha ett annat förhållnings-sätt för de har ju andra utmaningar. Jag tycker ändå Sverige har kommit en bra bit på vägen men vi är ju inte lika långt som exempelvis Tyskland och England som har haft betydligt hårdare regler och lagar på loggningen. Det är där som är den största utmaningen som jag ser. Hur loggar vi, hur följer vi upp, och vem ansvarar för loggningen. Så utbildning kommer vara en sak sen tror jag också massmedia kommer göra detta till att det blir upphöjt till en medial fråga. Då kommer också frågorna börja komma. Så utbildning i all ära, för den kommer vi kunna ha Men när man däremot pratar men vänner och släkt så är det en väldig skillnad hur man bedriver det i och med olika företag. Därför finns ju inte den här totala förståelsen. För att jag kan svara om två tre år så är det för att vi själva också förstår bättre vad lagen kommer att innebära Just nu är lite som att sätta upp finger i vinden och kolla vart det blåser.
IP2.17	I:	Om man då tittar i allmänhet, har det skett någon sådan där större förändring som kan vara både informationsrelaterad men också säkerhetsrelaterad?
IP2.18	K:	Ja man gjorde väl en förändring om jag inte missminner mig -96 när nya patentlagen inträdde. Då var det också en förändring När man skärpte lagarna med Pal och PUL då blir det i alla fall en upphöjning av de tidigare reglerna. Annars kanske man kan jämföra GDPR lite komiskt till millennieskiftet när alla datorerna skulle ställas om och världen skulle gå under. Det är det här som är lite utmaningen, på vilken nivå ska man lägga detta? Det som är allvaret i det är ju konsekvensen. Jag tror vi upprättar GDPR på ett relativt bra sätt I det avseendet att vi har lagar som styr ganska tydligt vad vi måste göra och inte göra. Konsekvensen är ju snarare den här betalningsdagen, straffbeläggandet på fyra procent. Om vi inte har förstått rätt eller jobbar i de riktlinjer som kommer stipuleras, det kanske man vet först när EU-domstolen kommer ha ett prejudikat.
IP2.19	I:	Om vi går vidare till awareness, hur går ni på Unilabs tillväga för att informera anställda om GDPR?
IP2.20	K:	Just nu så sker det egentligen en kanal som vi använder oss av mycket, workplace. Det är den här Facebook at work. Där lägger vi ut regelbunden information om den, samtidigt som det ju inte är någon som vet vem som läser vad. Så vi har inte gjort någon aktiv utbildningsplan i nuläget av den anledningen av att vi

		är fortfarande i en Gap-analysfasen och innan den är klar och vi vet vad som görs på ett bra eller sämre sätt, vilka luckor vi måste täppa igen så kommer ju inte en utblandning ske innan dess. Det innefattar ju en större plan.
IP2.21	I:	Så då har ni i dagsläget inga planer då på utbildningar, föreläsningar eller praktiska moment?
IP2.22	K:	Det finns i planeringen, men det finns ingenting som är utrustat nej.
IP2.23	I:	Så då har ni tittat på på vilket utplägg man kan tänka sig ha på utbildningar?
IP2.24	K:	Från ett personligt perspektiv nej. Det har jag inte varit inkluderad i men jag är fullständigt medveten om att Bird & Bird egentligen är ett av de ledande företagen som är rådgivande företag för Unilabs, samarbetar ju ur ett Group-perspektiv i denna frågan. Det kommer säkerligen ske en hel del aktioner när vi närmar oss, parallellt med den här Gap-analysen som vi gör där. Idag har vi inget aktivt, vi avvaktar vad vi ska göra.
IP2.25	I:	Om man ser på information till de anställda om GDPR, är det något som de kommer få en gång eller som kommer inkluderas som en kontinuerlig process?
IP2.26	K:	GDPR kommer bli som ett Culture behaviour skulle jag vilja säga. Vi har något som heter mission motto-mantra, culture building behaviours topics som vi jobbar med dagligen eller i verksamheterna. Jag tror en GDPR kommer bli en culture behaviour. Det handlar ju som om att förstå hur patentlagar och så vidare, det kommer ju vara en naturlig del av vår vardag. Det är ju någonting nytt [syftar till GDPR] och det kommer innefattas i de dagliga rutinerna Det vi gör idag är ju snarare att informera om att GDPR kommer komma inom en APT och som sagt i workplace och så vidare. Så att man känner igen namnet bara och vet vad det är. För tre fyra månader sedan så var det kanske ingen som visste vad ordet GDPR betydde egentligen. Idag kanske man har en kännedom om vad förkortningen är i alla fall. Men innebörden tror jag kommer vara ett konsekvent arbete.
IP2.27	I:	Anser ni på Unilabs att det är viktigt att medvetandegöra GDPR för de anställda?
IP2.28	K:	Jag anser att det är väldigt viktigt, sedan är det kanske omfattning av den, det är kanske där som det skiljer sig åt beroende på vem du pratat med. Att man kanske inte förstått innebörden i omfattningen, som att man inte vet av innebörden är fullt ut. Så konsekvensanalysen kommer lättare att göras när vi får bättre riktlinjer i det hela Men från mitt perspektiv så är det ett jätte viktigt topic att prata om. att förmedla och ha med vid mötena med medarbetarna men även med kunder. Kunder internt sett, men också externt, kunder som vi har som leverantörer också eller där vi är kunder till.
IP2.29	I:	Hur gör ni då för att medvetandegöra GDPR?
IP2.30	K:	Vi har tryckt upp en massa t-shirts... nä men i det fallet så lyfter vi det i samtalen när vi träffar leverantörer i leverantörsmöten så är det GDPR en punkt som jag lyfter i de samtalen för att veta också var de står i frågan och för att få kunskap. På samma sätt som ni genomför den här intervjun genomför jag intervjuer med leverantörer för att få en medvetenhetsgrad, vilken nivå vi ligger på och hur de jobbar. Hur vi kan ställa våra förväntningar jämfört med dem. Våra kunder, beroende på vilka som är våra kunder har också kommit olika långt så de bör ju ställa kvar på oss. I samtal med medarbetarna, återigen att medvetandegöra det dagliga. När GDPR kommer bli en hype, det kommer det bli den 25e maj så kommer ju komma tusen frågor vad det innebär för en själv. Vilka risker och vilka rättigheter har jag också vidare. Så därför att avdramatisera det genom att vi jobbar med det. Men att vi då kanske inte har en fullständig actionplan är en annan sak men att vi medvetandegör ämnet.
IP2.31	I:	Vad tänker du och höger upp i organisationen att ni vill uppnå med att medvetandegöra GDPR?

IP2.32	K:	Jag tänkte säga, varför alla företag gör detta, det finns väl bara en anledning egentligen om man kan hårdra det. Det är ju för att man inte vill riskera fyra procent i skadestånd. Det är väl rent krasst den sanna verkligheten. Sen att vi då också i verkligheten vill uppfylla GDPR förutsättningar i vår verksamhet det är ju självklarhet. Men det är väl straffbeläggandet som ingen vill ha.
IP2.33	I:	Och just när det gäller förändringar i den dagliga verksamheten eller överlag, har du fått någon respons från personal om vad dem tycker om det här?
IP2.34	K:	Ska vi tycka någonting om GDPR tänkte jag säga, den kommer komma oavsett vad. Nej men så införandet, i och med att vi liksom inte aktivt jobbat med det på det viset ut gentemot medarbetarna i nuläget, så det enda vi kan egentligen återkoppla till både externt och internt är egentligen att vi har en planering som vi förhåller oss till, att vi är i nuvarande skede i en GAP-analys, att som personligen kan jag tycka att vi är sent ute men om jag jämför med många andra så är vi även också tidigt ute, men det finns dom som har kommit betydligt längre. Så det är snarare hur kan vi komma ikapp i det arbetet för att liksom kunna genomföra resterande implementeringen. Sen är det så GDPR är inget slutdatum på den 25 maj, utan 25 maj är en början på det och det gäller att ha en handlingsplan hur vi ska täcka de kommande 2 åren. För det kommer vara en lång process i detta. Så det är det som jag brukar använda som ett budskap, att vi är igång, vi jobbar med det och vi kommer då liksom att kunna se det som en kulturförändring som vi måste göra.
IP2.35	I:	Och hur tar de anställda emot just det här med att det blir kulturförändring för dem inom organisationen?
IP2.36	K:	Återigen, den kan jag svara bättre på i höst för då har vi kommit lite längre och då vet vi liksom lite mer vilka krav som ställs. Jag menar om ni skulle gå och fråga gemene man på gatan vad GDPR är utan att veta bättre, så skulle jag bli väldigt förvånad om alla säger: Att det där vet jag fullständigt vad det innebär. Det är snarare nu om man ska slå det här med Facebook till exempel som händer ur ett GDPR perspektiv, då är det snarare Facebook som är dåligt om man ska säga det man relaterar till, inte att GDPR lagen och så vidare. Den medvetenheten den ger där kommer komma inom media tror jag och det är där frågorna kommer att uppstå. Konsekvenser och förändringar tror jag det kommer uppkomma efter hand som implementeringen sker, frågorna uppstår.
IP2.37	I:	Om man tittar rent överlag när det gäller så här stora policyförändringar, inte bara GDPR utan rent generellt, har ni någon standard för hur ni medvetandegör sådana stora förändringar till de anställda?
IP2.38	K:	Jag kan säga så att peppar peppar så sker inte så här stora förändringar standardmässigt eller rutinmässigt varje år. Att det blir förändringar i lagar eller förordning eller blir en justering, det jobbar vi standardmässigt med, men det är inget man kan säga att vi har en rutin för hur man ska hantera en GDPR situation. För den är så pass omfattande, så att det är snarare att vi förhåller oss till vad måste vi göra i nuläget utefter den här förutsättning och lite som svar på din fråga man uppfinner hjulet en gång till då.
IP2.39	I:	Jag tänkte på just det här du sa om kultur och att det blir en kulturförändring, har man gjort något liknande förut och hur har man gått tillväga då för att implementera något i kulturen?
IP2.40	K:	Det var en bra reflektion, vi har gjort en kulturförändring så sent som bara 2 år sen när vi började prata om mission motto mantra och culture building behaviour topics. Och då hade man en införandeprocess i det och om vi tar det som en lärdom, så tror jag absolut att processen hur vi rullar ut en utbildningsplan, hur vi rullar ut informationen, att vi har liksom i de fallen samarbetspartners som känner till oss och kan trycka materialet och så vidare. Att vi kan ha en likhetsfaktor i det, så utifrån det tror jag absolut att vi kommer ha en förenklad process i utrollningen av det. Men det jag mest menar är att jag tror inte att det finns en standard hur man hanterar en GDPR fråga i det, men det är snarare utifrån en lärdom för hur vi måste få ut så har vi en process för det internt sett.

IP2.41	I:	Har du någon uppfattning om den generella nivån om just medvetenhet kring informationssäkerhet och just patientdatalag och liknande som finns bland medarbetare idag?
IP2.42	K:	Jag tror utifrån var och en person så är det ju väldigt subjektivt för det första, men jag tror samtliga medarbetare som jobbar inom hälso- och sjukvård har ju ett ansvar om inget annat så vet de ju vad sekretess betyder. Att man ska behandla patientinformation utifrån de förutsättningar lagen stipulerar och sunt förnuft, så det här vardagliga sitter ändå i ryggmärgen i vår kultur inom hälso- och sjukvård sedan många år tillbaka. Däremot tror jag liksom det som GDPR stipulerar som inte finns i patientlagar det är ju att det är inte GDPR har ingen patientrelation utan den har en personrelation och jag tror det är där som den största förändringen ligger att vi ser inte kanske alltid personen, vi ser patienten. Och vad är persondata istället för patientdata, det räcker till exempel inte att stryka över ett personnummer och fäxa en remiss och sedan kan man ringa och berätta personnumret, nu blir det ju att du kan ju inte ens fäxa överhuvudtaget om man ska hårdra det utan att du loggar det. Det är den där dimensionen att persondata är faxningen, så jag tror det är där den stora förändringen kommer ligga, att förhålla sig till detta och inte slentrianmässigt jobba bara med patientdata, men för den sitter i ryggmärgen. Den föds vi med inom skolan tänkte jag säga och i vår vardag.
IP2.43	I:	Om man då just tittar på informationssäkerhet, är det någonting liksom i det dagliga arbetet som man gör för att få medarbetarna att vara medvetna om hur man ska jobba med informationssäkerhet för information inte ska hamna på fel ställe?
IP2.44	K:	Unilabs är ett ackrediterat företag, det är vi och Lund/Malmös universitetssjukhus. Så i vår ackreditering och dokumentering finns stipulerat hur man ska hantera de här frågorna gällande patientdata framförallt. Vi har en informations säkerhetsansvarig person som jobbar med det, så att i det normala flödet så ser jag ingen omedvetenhet i det, det är snarare hur vi förhåller informationssäkerheten till GDPR som kommer vara den stora förändringen och återigen att informationssäkerhet ser vi ofta som patientdata. Det är samma som nu till exempel inom röntgen som jag jobbar med, då är det ju att låt säga att du röntgar en felaktig patient eller låt säga du röntgar rätt patient men bilderna hamnar på fel ställe. Idag gör man en korrigerig om man medvetandegör det, då gör man en riskbedömning är jag säker på att de här bilderna är denne patients och då flyttar jag över dem till rätt mapp. Skulle det vara en riskbedömning, låt säga att jag är inte säker på att de här bilderna är rätt överhuvudtaget, då får jag kalla tillbaka de här patienterna och röntga om. Skillnaden är ju egentligen där att om jag är säker, jag flyttar över så finns det ju ingenting mig veterligen som informationsmässig plikt att informera patienten om att man begått ett fel eller att jag gjort en korrigerig/rättelse. Men med GDPR så finns det stipulerat att jag måste meddela patienterna som det berör inom 72 timmar och det är en helt annan hantering i risk management och i dem här ärendena. Vad den fyller för funktion i praktiken låter det jag vara osagt, men vi måste ju ha en hantering som reglerar det. Så där är väl en skillnad när det gäller informationssäkerheten att hur vi medvetandegör det gentemot GDPR. Det är samma sak som en hantering som att radera bilder, att vi måste ha en process att vi inom en månad måste kunna [Uppkopplingen tappades, frågan ställdes igen] Idag kan man säga i telefon att vi kan inte radera dina bilder, men med GDPR måste vi ha en process som ger det faktiskt att vi måste kunna hänvisa till att du måste göra en ansökan och att vi kan bevilja eller inte bevilja den ansökan, så det är snarare den process hanteringen som kommer att skilja sig i informationssäkerheten.
IP2.45	I:	Det du pratade om just det här att röntga rätt patient som hamnar på fel patient i systemet, har ni något sätt ni gör när just sånt här händer för att göra de anställda medvetna om det här har skett men helst ska det inte ske så att säga?
IP2.46	K:	Återigen så tror jag om vi vinklar om frågan, vem är det som gör fel? Det är ju medarbetaren själv ju, inte egentligen någon som medvetandegör det till organisationen att det har blivit en felaktighet och då har vi ju i det fallet en avvikelshantering som vi använder ett system som heter Flexsite och där har vi klara rutiner för hur en avvikelse ska skrivas, hur man hanterar det och i det fallet hur man behöver eskalera det om det är liksom beroende på vilken typ av avvikelse

		det har varit, vi gör en gradering på 1-4 det görs inte av medarbetaren själv utan det görs i det fallet av operativa chefer och till syvende sist av sverigechef och kvalitetschef. Så vi har en intern process för avvikelsehantering som alla är fullständigt medvetna om. Sen har man ett personligt ansvar ju att skriva detta, vi kan ju inte tracka att det har blivit fel om inte felet flaggas upp. Så det vi gör i det fallet är att trycka på processen mer, att man har ett ansvar att vara en del av process.
IP2.47	I:	Har du personligen varit involverad i något annat projekt eller program som har haft med medvetandegörande av just informationssäkerhet?
IP2.48	K:	Mer än i mitt verksamhetsansvar och driftschefs ansvar menar du?
IP2.49	I:	Ja, eller i det ansvaret också.
IP2.50	K:	Jag har haft personalansvar och i personalansvar innebär det att man får en introduktion och man måste medvetandegöra alla regler och lagar som finns. Vi har protokoll att följa vid APT så att man pratar om ansvar fast på många olika plan, informationsansvar är ju en del av det och att man liksom i det fallet till exempel som en sån sak att man märker på rätt sätt och att man liksom tänker på att man väljer rätt patient, att man när man fått en avvikelse och hanterar det så måste man informera och återkoppla och se om man i det fallet göra en förändrad rutin eller ge utbildning, hur förtydligar vi det. Så utifrån det har jag absolut varit inblandad i det, om det gäller större förändringar enligt regelverk så beror det på vilken typ av information vi pratar om.
IP2.51	I:	Jag tyckte svaret du gav svarade bra på just den frågan.
IP2.52	K:	Då förstår vi varandra vill jag säga.
IP2.53	I:	Tycker du att vi missat att fråga dig om något under denna intervjun eller är det något du velat trycka på extra?
IP2.54	K:	Jag tycker frågorna är jättebra, det är tydligt att de är riktade, vad vi gör gentemot medarbetarna, det som jag kan känna som kanske skulle varit en intressant sak att ta med sig i det är innan vi kommer så långt är det snarare hur jobbar man inom både mot offentliga och privata sektorn med GDPR, i informationen mellan varandra också. Det kanske är en avgränsning vill jag säga och kanske en medveten avgränsning, men det finns en väsentlig skillnad hur vi jobbar faktiskt med GDPR gentemot privata aktörer och offentliga sektorn, det är liksom som passus det är sån här GDPR nörd som en annan som tycker det kan vara jätteskoj att prata om. Men just offentlig sektor kan jag säga det är väldigt lik information därifrån, jag tar ju oftare i hand med den privata sektorn för den är ju väldigt aktuell där, där märker jag en jättestor skillnad, det samma när jag pratar med kollegor eller vänner i bekantskapskretsen så märker man en väldigt skillnad vem som jobbar i offentlig sektor och vem som jobbar i privata sektorn.
IP2.55	I:	Du menar utifrån ett GDPR perspektiv?
IP2.56	K:	Ja, utifrån GDPR perspektivet.
IP2.57	I:	Har det att göra med medvetenheten kring GDPR eller har det att göra med hur man jobbar med GDPR?
IP2.58	K:	Good question, för jag tror inte att offentlig sektor om man ska generalisera nu drar jag alla över en kam, jag vet att region Skåne har kommit en bra bit på vägen jämt mot många andra landsting. Men däremot får jag uppfattningen i alla fall att man inte har medvetandegjort det så tydligt hos medarbetarna och fast man är en processor eller till stor del en controller i mångt och mycket så jobbar man väldigt mycket internt inom sin region, men man glömmar i mitt tycke att räcka ut handen och säga att vi kan hjälpa er eller vi vill ha er hjälp i den här frågan, man löser det väldigt mycket inom sitt område. Den privata då är det mycket mer att alla söker just nu svaret på ett annat sätt och ställer också krav på varandra mycket tydligare, vad har ni gjort, vart har ni kommit, vi behöver er hjälp, vi behöver er återkoppling, det är lite mer panik faktiskt inom den privata

		sektorn för att ingen vill riskera att hamna under luppen i just för att behöva böta 4 procent. Medans den offentliga sektorn så får man snarare nu får ni citera mig som ni vill: men det känns som att det är inte mina pengar, så jag kan inte bli ansvarsskyldig för det ändå och vem ska jag kunna gå på staten? Vem är det som pliktar för att man inte uppfyller GDPR reglementet, så där har vi kanske lite olika nyanser i hur vi förhåller oss till GDPR. Det är en passus.
IP2.59	I:	Det är jätteintressant, vi har haft intervjuer också med Region Skåne till exempel och kommer ha flera även där. Så det är jätteintressant att få olika perspektiv på det hela.
IP2.60	K:	Intressant är om ni gör en uppföljning om ett halvår, för då vet vi kanske lite bättre vart vi står och vilka utmaningar vi har mött, jag tror att det är bara början detta på en större kulturförändring i samhället också. För mig är det väldigt mycket större än vad jag tror det allmänt uppfattas som.
IP2.61	I:	Vi tackar för intervjun och överlämnar en liten gåva som tack för deltagande.

Appendix 4 – Intervju 3

Organisation: Vuxenpsykiatri i Malmö och Trelleborg

Intervjupersoner: Jenny Rundberg

Per Granvik

Yrkesroll: Verksamhetsutvecklare

Tid och plats: 13.00-14.00, tisdagen den 17 april 2018, personligt möte i Malmö

I: Intervjuperson

J: Jenny

P: Per

Referens	Respondent	Frågor och svar
IP3.1	I:	Kan ni berätta lite om er roll här på arbetsplatsen?
IP3.2	J:	Vi jobbar med samma sak, som verksamhetsutvecklare båda två, det innebär egentligen att vi kan få uppdrag av verksamhetschefen kring nästan precis vad som helst. Ibland är det ju som det här, ett visst projektarbete som ska genomföras och så.
IP3.3	P:	Ja, det spretar ju åt lite olika håll och det går ju lite i vågor, men jag har vissa fasta saker som jag fortfarande håller på med. Inflytandearbetet "Mina planer" som förhoppningsvis ska kunna ta slut, så har jag lite kring NSP och införandet av både urskrivnings-guiden, patientforum, support och inflytandearbete. Sen har jag några övergripande uppdrag som inte tar så jättemycket tid.
IP3.4	I:	Hur länge har ni båda jobbat är?
IP3.5	P:	I huset eller inom psykiatri?
IP3.6	I:	Med den rollen ni har nu?
IP3.7	P:	I den rollen, ja från och till. Jag har jobbat på psykiatri sedan 80, men rollen som verksamhetsutvecklare, ja från och till. De senaste tre åren kanske, egentligen bara två år för innan hade jag chefsuppdrag, ja, svårt att säga.
IP3.8	J:	5 år.
IP3.9	I:	Hur har förberedelsema inför GDPR sett ut?
IP3.10	J:	Ska du ta den?
IP3.11	P:	Ja det kan jag i och för sig ta. När den kom, det är ju någon månad sedan vi blev uppmärksammade på det, det gick ut till divisionen om att det här ska vi fördjupa oss litegrann i. Vår verksamhetschef delegerade ner det till oss och sa att det här får ni fördjupa er i. Vi fick börja med att läsa på lite. Sedan är det någon på vår förvaltning som har huvudansvar för förvaltning, Skåne Sund.
IP3.12	J:	Margareta Johansson hon är övergripande ansvarig för hela den här förvaltningen.
IP3.13	P:	Så då började hon strukturera upp som det här initialt det här ska innehålla, i form av både information utbildning, PowerPoint och vi har fått en del Skype-information, Skype-utbildningar kring vad lagen innebär. Det har väl pågått en tid, men framförallt information i första skedet och sedan mer specifikt uppdrag kring

		inventering. Sedan vilka system som vi ska lämna till förvaltningsnivå, de system där vi inte är inne o tittar i utan det är på förvaltningsnivå Melior och så vidare.
IP3.14	J:	Det började här nu i januari så var det Margareta som tog kontakt, att Hans (verksamhetschef) fick veta att nu är det här arbetet genomfört och att vi blev kontaktpersoner och att det ska genomföras inom verksamhetsområde. Det är väl 850 anställda fördelat på ett 40-tal. Då informerade man vid ett tillfälle för hela ledningsgruppen, LEG, då som är områdescheferna, sen var ju hon med oss och informerade till alla enhetschefer på deras ledningsgruppsmöten där områdescheferna och enhetscheferna sitter. Psykiatrin har ju fyra områden med ett visst antal enhetschefer inom varje område då. Så då fick ju alla den informationen och sen har ju det faktiska arbetet med att göra inventering den sker ju på plats, det får ju var och en göra, men enhetschefen har i uppdrag att ansvara för det på sin enhet och sen så ska de sammanställa det och skicka det till oss. Så vi kan sammanställa det för hela verksamhetsområdet då. Det är vi i slutampen på nu så på fredag bör vi vara klara.
IP3.15	I:	Vad kommer ni göra med den informationen sen?
IP3.16	J:	Den lämnar vi bara vidare till Margareta, så sammanställer hon för hela Skånevård Sund, utifrån vad det då ger, så kommer de arbeta vidare med vad är det så man ser, vad är det för information som finns, är det IT lösningar som behöver göras för att vi ska kunna spara de [filer] på ett säkert sätt.
IP3.17	P:	Det är ju två spår där, vad kan gå in i befintliga system? Behöver vi ha just den här listan? Eller går den att få in i något som vi redan använder. Det andra är, hur kan vi skapa en säker plattform som du måste ha som arbetsdokument i våra burkar och hur gör vi det på ett säkert sätt. Men där är inte vi än. Information, inventering och sedan upp med den i hierarkin.
IP3.18	J:	Och sen få folk att städa.
IP3.19	P:	Våra gemensamma system som vi har vi varit inne och tittat i och städlat lite grann.
IP3.20	I:	På vilket sätt tycker ni att GDPR har påverkat er och era arbetsuppgifter?
IP3.21	J:	Det har ju påverkat på det sättet att vi är kontaktpersoner och jobbat med fråga och gått ut med och informerar och fått olika frågor och så kring detta. På det sättet är det ju en direkt arbetsuppgift vi har att försöka verkställa detta nu i hanteringen och rensningen. Sedan i våra egna andra professioner så har det väl mer medfört att vi titta på vad har vi själva för dokument och rensat det som har behövts där.
IP3.22	I:	Har det på något sätt förändrat ert arbetssätt som verksamhetsutvecklare?
IP3.23	P:	Det har inte gjort det än, detta är ju ett uppdrag som för att göra inventering och spridning av information. Sen vad själva lagen de facto innebär är och hur det påverkar oss i vår vardag. Det har vi inte sett än i den bemärkelsen. Sen tror jag inte vi har jättemycket, du har ju en del dokument men väldigt lite av den typen som påverkas av den nya lagen. Jag har ju inga listor på patienter eller så.
IP3.24	J:	Jag tror det påverkar en så, när vi har pratat med enhetschefer och andra anställda så märker man att det har ju påverkat väldigt mycket i den här medvetenheten. Att man inte kan stoppa in och spara grejer där och sedan är det glömt och säkert, dels att vi inte ska spara saker som vi inte behöver längre och att vi ska verkligen använda oss av de befintliga systemen och man ute på enheterna har börjat tänka efter väldigt mycket med, på vad har vi egentligen och varför har vi detta? Kan vi då ha det på något annat sätt? Ibland blir man osäker men det kan vi kanske men inte som vi känner till. Eller ibland har man mer kunskap och det går inte i de systemens om vi har. Så jag tror vi har det genomgående fått folk att reflektera kring varför man har personuppgifterna sparas.
IP3.25	I:	Vad tror ni det är som krävs för att ni ska kunna följa förordningen?

IP3.26	J:	Jag tror vi har det ganska bra, det kändes inte, jag är nog förvånad över att det inte är mer. Den kritiken som kommer fram det är väl att man behöver ha något tydligare system när det gäller, Vops exempelvis som är ett IT-system som vi använder oss av idag som är ganska så svårtypligt och men kan inte ha tillräckligt många uppgifter som man skulle vilja ha ute på enheterna och använda det som en snabb överblick och så.
IP3.27	I:	Vad är det för program?
IP3.28	J:	Det är ett bokningssystem kan man säga. Vi har ju ett behov av att ha lättillgänglig information över patienter, de här är inlagda just nu, de har detta och den här kontaktpersonen. Det kan man känna ibland att de systemen som är för svårtypliga för det. Så kan man skapa det utanför.
IP3.29	P:	Det andra tänker jag att det är en del sådana här listor som dyker upp i inventeringen som man ser då, att det går inte att få in i våra befintliga system som man behöver i det dagliga arbetet. Utan där kan jag ha förhoppningar om att vi får någon form av säker yta i våra IT-system att lagra den typen av information som vi behöver jobba med dagligen utan att riskera att det far iväg. Utan någon form av säker lagringsyta.
IP3.30	J:	Att den informationen som har kommit fram från oss som ligger utanför systemet. Det har alltid varit temporära saker, det här är ett aktuellt arbetsmaterial det är ingenting vi spara i årtal utan det är uppdateras hela tiden. Men just nu ser det ut såhär och det vill jag kunna veta. Exempelvis de här patienterna har jag i stödsamtal och så vill jag ha en lista på deras namn och hur ofta jag ska träffa dem för att kunna veta det snabbt. Annars finns det risk att jag tappar någon. Då missar jag att Maja har jag inte träffat. Så att det är den typen listor som jag tycker att man sett mest av. Där man känner att man inte vet vart man ska ha det här på ett lätt.
IP3.31	I:	När man ser det här med inventeringen och sådant, efter den, vad tror ni blir den största förändringen i den dagliga verksamheten i och med GDPR?
IP3.32	P:	Den största förändringen tror jag är en ökad medvetenhet hos personalen. Om vad det faktiskt är för uppgifter vi ska spara och var vi sparar dem och hur vi sparar dem. En större medvetenhet om sekretessregler som gäller och att en patient faktiskt har rätta att kräva ut vilka register denne finns i. Det är väl min förhoppning, en större försiktighet om hur vi hanterar känsliga uppgifter.
IP3.33	I:	Ser ni att den berör alla inom organisationen eller bara vissa yrkesgrupper?
IP3.34	J:	Alla
IP3.35	P:	Alla, sen är det vissa som är drabbade mer än andra men jag tror att på ett eller annat sätt blir alla berörda.
IP3.36	I:	Är det några yrkesgrupper som blir påverkade mer? Och på vilket sätt?
IP3.37	J:	Cheferna i sådana fall
IP3.38	I:	Vilket sätt skulle det påverka dem då?
IP3.39	J:	Jag tror dem oftare sitter på mer information, sen har ju de mer personuppgifter och sådant också som de sitter på.
IP3.40	P:	Att de oftare får ta hand om de svårare klagomålsärendena, folk som är missnöjda som man ändå behöver ha koll på. De får mycket korrespondensen från både patienter och anhöriga, kring både klagomål, eller som i alla fall innehåller uppgifter och av känslig art som de då måste hantera De blir nog mer drabbade än andra. Så cheferna gäller naturligtvis både områdeschefer och verksamhetschefer.
IP3.41	I:	Vilka utmaningar finns inom psykiatri i och med GDPR?

IP3.42	P:	Jag tänker ju att den stora utmaningen egentligen är att få alla 850 medarbetarna att faktiskt gå igenom sina, jag menar vi kommer ju inte ha en chans att gå igenom allas egna kataloger. Varje enskild medarbetare har inloggning med kort, har ju sin egen katalog och sina egna dokument sparade på lite olika ställen. Den stora utmaningen blir ju att få ut den informationen och vikten av att göra den där inventeringen. Gällra slänga gamla filer, utan möjligheten att faktiskt gå in, man kan ju göra stickprov möjligtvis, men gå in i varje enskild 850 och så 3000 för hela psykiatrin medarbetare det är väl utmaningen. Att vi inte kommer att ha full koll.
IP3.43	I:	Tror ni att, på något sätt behöver ändra tankesättet och kulturen bland de anställda?
IP3.44	P:	Ja. Det tror jag nog att vi kommer, en ökad medvetenhet, vi att lyckas skapa. Min förhoppning är ju också att vi ska kunna erbjuda någon form av lättbegriplig säker yta att spara på. Att få in den rutinen tror jag blir lättare. Så här gör du när du har känsliga uppgifter eller listor, du spara dem där. Där är de säkra där man kan logga in, har man de så tror jag det är lättare att leda in folk att det är där ni ska spara det. Allt som är känsligt sparar ni där. Då framledes, är väl förhoppningen att vi får ordning på det här.
IP3.45	J:	Det är ju mer en utmaning uppåt. För det är ju inte vi inom psykiatrin som ska ta fram de systemen som behövs eller göra förenklingar i befintliga system som att de skulle bli mer lättanvända.
IP3.46	I:	Om man tittar på era tidigare roller, har ni varit med om när det var någon så här stor policyförändring som är informationsrelaterad eller som har med säkerhetsrelaterat eller att det blivit lagändringar?
IP3.47	P:	Ja, jag har ju parallellt en annan, det handlar ju om Mina planer, där vi fick en ny lag nu från 1/1 kring hur vi ska samverka med kommuner hur vi ska kommunicera med varandra. Det är ett IT system som ska användas. I kommunikation mellan kommun och landsting. Där den nya lagen ställer förnyade krav, den är på något sätt jävligare, den är besvärligare där vi har 33 kommuner också som ska samverka. Här har vi ju egentligen i någon bemärkelse en tydlig uppgift som, information, inventering sedan får någon annan lösa det tekniska på övre plan.
IP3.48	J:	Jag tyckte en stor förändring, men det är ju jättelänge sedan, när man gick från pappersjournal till digital journal. Det var ju en väldigt stor förändring, med förändring i arbetssätt, säkerhetsmässigt. Det var ju mycket diskussioner då kring hur hänger detta ihop.
IP3.49	P:	Där har vi ju en ännu större utmaning längre fram men den sammanhållande digital miljö vi ska byta journalsystem i hela Skåne. Men den tiden.
IP3.50	I:	Ser ni några samband nu med det ni sa och GDPR?
IP3.51	J:	Lite spekulationer, men då var det ju som om man kände att man ägde sin journal, det var ju brandsäkra rum som alla pappersjournalerna stod i och så sattes det in där och där kändes det som om man hade koll, det var ingen annan som kunde ta sig in där. Sen blev det den här osäkerhetskänslor när allt nu bara ska in i en burk och var ligger det och, hur säkert är det? Det var ju mer amatör-mässiga funderingar. Sen så kanske det slår över tills man tycker att det är så pass säkert, att man inte tänker på att man lägger in mycket och sparar väldigt mycket och att det kanske blir en dumpningsplats. Ja det är ju sparat i datorn, det är ju säkert. Till att nu GDPR säger att det ska vi inte alls, utan nu ska det rensas nu ska ni bara ha det ni måste ni ska verkligen ifrågasätt om ni verkligen behöver den här informationen och var den förvaras, så kanske lite så Wake up call i det.
IP3.52	I:	Då när det gick från pappersjournaler till det digitala var det några problem som uppstod?

IP3.53	P:	Klart det var massor av problem. I den bemärkelsen att det var införandet av ett nytt system men alla de brister som det innebär att hacka och så. Också naturligtvis problem med tilliten till det i personalen att det var mycket med information och tillit att det faktiskt finns en digital miljö. Det där tar ju tid, det är ju fortfarande dem som blickar tillbaka med en viss nostalgi och tycker om vi ändå kunde få tillbaka pappersjournal. Men allt förändringsarbete finns det ju motstånd mot, det finns ju alltid en grupp som tycker att det är svårt med förändringar.
IP3.54	I:	Var det något speciellt man gjorde då, för att hantera det här motståndet?
IP3.55	J:	Det var ju inte så mycket att välja på. Nu är det så här och så, det var ju mer utbildningsinsatser om hur det ska göras och sen att vissa enskilda kanske behövde mer stöttning i hur det skulle göras och kanske inte hade sekreterare som skrev åt sig och så och hade svårt med det. Men det var ju liksom inget man kunde välja. Det är ju inte detta heller. Det är ju en lag att förhålla sig till.
IP3.56	P:	Det man gör egentligen i allt sådant förändringsarbete det är att skapa någon form av struktur på hur vi ska få ut informationen hur man ska få följsamhet till det och rapportera tillbaka den strukturen finns där ju. Vi som på verksamhetsnivå har ju något som av implementeringsansvar sen finns det ju alla enhetscheferna utåt och kanaler uppåt. Att det blir en ständig nerrapportering och upprapportering, den strukturen måste finnas i allt försäkringsarbete. Där man skapar forum för det, och utbildningstillfällen, här har det mer handlat om information men vissa utbildningstillfällen tillsammans med Melior då, där man kan öva digitalt på hur man ska använda det här och det här. Ibland kanske både lite moröt och piska att se till att det här faktiskt skall genomföras. Det är inget vi kan välja bort utan du måste göra den här utbildningen. I en digital miljö för att kunna använda ett här redskapet som vi nu ska använda. Så ibland är det så, det här ska vi bara göra. Där finns ingenting annat.
IP3.57	I:	Om vi går över då till det här med att medvetandegöra, hur går man tillväga inom psykiatri för att informera om GDPR?
IP3.58	J:	Först informerades det då för [NÅGOT] för områdescheferna och sedan så informerades inom varje område till enhetscheferna, då togs det fram också särskilda material som dels ett material som var lite mer omfattande som var det materialet som till enhetscheferna och sedan ett annat material som togs fram till enhetscheferna som i de i sin tur skulle använda sig av för att informera sin personal Så det har ju vi fått hjälp av med Margareta att hon har tagit fram, det materialet som ska gå ut, sen har vi också mailat ut till alla chefer och alla anställda kring hur det här berör dem.
IP3.59	P:	Du har ju suttit med några enhetschefer och gjort inventering tillsammans med dem för att se vilka de enhetscheferna hade och skickat ut det till andra enhetschefer, det här var vad vi hittade på de här två enheterna, har ni något mer? Eller är det ungefär samma typ av dokument? Då har ju enhetscheferna nått in materialet från sina anställda som har sagt att jag har det här och det här.
IP3.60	I:	Finns det några planer på hur man ska lägga upp framöver med utbildningar, föreläsningar och liknande?
IP3.61	J:	Jag vet att det är planerat, jag vet att dem planerar att det ska finnas som en webbutbildning men inte som vi har tagit fram här, men jag vet att det planeras från divisionens sida.
IP3.62	P:	Så det kommer väl, när det väl kommer. Men det är inget vi gör utan det görs på högre nivå så får vi försöka få ut det.
IP3.63	I:	Så då är det en webbutbildning som kommer uppifrån då?
IP3.64	J:	Ja.
IP3.65	I:	Så det kommer inte vara där medarbetarna mer praktiskt får mer insikt i vad GDPR innebär?

IP3.66	J:	Jo, den kommer handla om det och personuppgifter och vad säger lagen, hur ska det sparas och så.
IP3.67	I:	Just det här med information om GDPR planerar man att ha det som en kontinuerlig process, där man diskuterar det under en längre tid och verkligen medvetandegör det flera gånger eller är det att de får informationen en gång och sedan ska dem kunna det?
IP3.68	J:	Jag tror det kommer bli en kontinuerlig process, det tror jag ju. Jag kan tänka mig man kommer ha mycket mer koll på det här.
IP3.69	P:	Jag har inte hört det men jag kan föreställa mig att det är något man får ha in i introduktionsprogrammet för alla nyanställda helt enkelt tillsammans med sekretesslag och annat sånt som man går igenom, så är detta väl nåt sånt som ska in där med.
IP3.70	I:	Anser ni att det är viktigt att medvetandegöra just GDPR för medarbetarna?
IP3.71	P:	Det är dryga böter om inte annat. Den ersätter ju PUL:en och det är klart att vi behöver ha en medvetenhet om vad det är för uppgifter som är lagrade och framförallt fundera på varför vi måste ha de. Så i någon bemärkelse kan jag tycka att det är lite viktigt att det här faktiskt når ut till alla medarbetarna, om inte annat ur ett mer allmänmänskligt perspektiv att jag själv skulle ju vara nyfiken på vilka register finns jag i. Jag har sett någon sådan sammanställning hur det normalt sett ser ut och det slutar inte med att man dör utan där fortsätter man figurera i x antal år som ökar efter ett antal år innan det sjunker naturligt dyker man upp i flera register. Visst är det bra att vi är försiktiga med hur vi lagrar uppgifter.
IP3.72	J:	Sen tror jag man är väldigt, eftersom vi jobbar i psykiatrin, är man redan så förinställd på att allting man hanterar och all information man får om det är muntligt eller skriftligt eller hur som, att det är sekretess och det är väldigt känsligt, så jag tror det finns en självklar mental beredskap så. Här är det med den tekniska delen av det.
IP3.73	P:	Vi har i alla år tjatat på folk framförallt när det gäller deras mejlbox som egentligen är en offentlig handling, att det händer inte allt för sällan att patienter mailar behandlare för att man hittat dem. Vi ska helst inte föra några som helst konversationer, får man då jobbiga besvärliga klagomåls mejl så ligger dem kvar lite för länge för att man är osäker på hur man ska hantera det. Man har tjatat rätt mycket om det där att du måste flytta dem därifrån, du kan inte ha känsliga uppgifter liggande i din mejlbox. Så en viss medvetenhet finns där redan tror jag.
IP3.74	I:	Tror ni det blir någon utmaning just att lägga in GDPR eller ni anser man är så pass förberedd i psykiatrin ändå så att man kan ta till sig det på ett lättare sätt än andra vårdenheter?
IP3.75	P:	Jag vill ju gärna tro det. I något perspektiv tror jag man tänker sig för samtidigt som jag också då känner att, vi har ju en del arbetsmaterial som man behöver ha på enheterna för att hålla sig uppdaterade, det är kölistor och det är annat som, så förhoppningen är att lagen ska skapa säkra system för oss att använda för vi kan inte sluta använda våra listor. Utan den stora utmaningen är högre upp så att säga, har vi bara säkra lagringsytor och säkra system så tror jag inte det kommer påverka jättemycket våra medarbetares dagliga arbete och ju mindre det påverkar så att säga ju bättre tekniska lösningar vi har ju lättare blir det att följa lagen. Utmaningen ligger snarare nu när man ska in och rota i gammalt som ligger där och skräpar, att få bort gammalt skit och sedan skapa nya säkra lagringsytor.
IP3.76	J:	Men det tycker jag med, utmaningen är den tekniska att faktiskt få till fungerande system och få till att de system vi har ska vara så smidiga att använda och vara så flexibla att man kan använda dem fullt ut.
IP3.77	P:	Ett sånt som jag vet att jag fått till mig är att vi har ett system som chefen använder när det gäller personal, problem med personal, sjukdom, så när personalen

		går och blir sjuk, rehab ärenden och sånt, så har vi ett system för sånt som heter artodocs, där lägger man in personal som är långtidssjukskrivna så följer man nån rehabprocess i detta. Men innan man hamnar där i så är det ibland att man kanske jobbiga samtal med sin personal som inte riktigt sköter sig eller som gjort nånting eller så också har man inledande samtal innan man hamnar i dem här systemen, det behöver man dokumentera någonstans och var sparar jag det och där vet jag att cheferna ibland har en del sådana uppgifter för att ha liksom ryggen fri att jag har haft det där samtalet om att nån personal var misstänkt berusad nått nattpass. Bara misstänkt och då vill jag ha samtal också måste jag dokumentera det. Det är inget rehab, personalen är inte sjukskriven men det här är ett samtal som jag ska kunna komma tillbaka till sen, jo men vi hade faktiskt samtalet och du sa och vi kom överens om, var t sparar man det. Visst man kan skriva NN också vet man själv vem det är. Den typen av lösningar behöver man skapa, chefen kommer alltid behöva ha en viss typ av dokumentering om personal, men även kanske också anhöriga som hör av sig anonymt, kanske inte anonymt om patienter.
IP3.78	I:	Vad tänker sig organisationen inom psykiatri att man vill uppnå med medvetandegörandet?
IP3.79	J:	Att följa lagen.
IP3.80	P:	Syftet är att vara följsamma till lagen, men naturligtvis också en säker hantering av medborgarnas personuppgifter, känsliga uppgifter ska hanteras på ett säkert sätt, det mäster vara syftet med det. Att vi naturligtvis följer lagen men för den enskilda medborgaren/våra patienters skull ska de känna sig trygga i att man hanterar alla uppgifter som finns där hanteras på ett säkert sätt.
IP3.81	I:	Och nu efter information som har gått ut om GDPR har ni fått någon form av respons från medarbetare på eventuella förändringar som behöver göras i deras dagliga arbete eller system?
IP3.82	J:	Det har vi fått.
IP3.83	I:	Har det varit motstånd eller hur har det mottagits?
IP3.84	J:	Det har mer mottagits, vi har försökt jobba för att man ska vara så öppen som möjligt, att det är bättre nu att berätta liksom vad ni har än att hålla tyst om det. Är det så att ni har ett system eller några filer eller så, berätta om det så vi inventerar det. Och det är väl mer motstånd där det har varit mer ta inte ifrån oss det här, vi behöver ha dem här uppgifterna för att kunna göra vårt dagliga jobb liksom och kanske nån rädsla i att man bara kommer gå ut resolut och säga att den typen får inte finnas punkt. Och att man då ska stå där och känna aha men vad ska vi göra då liksom, ska vi skriva ner allt det här för hand istället, då omfattas det inte av detta, men det är betydligt osäkrare att ha det liggande i pappersform någonstans. Mer den här rädslan i att det kommer leda till liksom den typen av beslut.
IP3.85	P:	Men det har vi försökt att vara ganska tydliga med när det gäller inventeringen, att de handlar inte om att förbjuda er att använda dokument eller personuppgifter utan det är mer att vi ska hitta säkra sätt att kunna lagra det på.
IP3.86	J:	Där verkligen många som skriver det här behöver jag, det här vill jag verkligen ha kvar.
IP3.87	I:	Finns det inom ert verksamhetsområde nån standard för hur man just medvetandegör för medarbetare om så här stora policy och lagändringar liknande GDPR?
IP3.88	J:	Kanske ingen sån uttalad inte standard så, utan mer att man försöker tänka efter så att informationen både kommer ut muntligt och skriftligt och att man försöker säkerställa sig att den verkligen når alla och att den också går rätt i linjen så folk vet var dem kan vända sig med frågor och annat. Så ett är väl en standard som man alltid försöker använda sig av när det är större.

IP3.89	P:	Alltså använda sig av linjen och strukturen som organisationen är uppbyggd kring och de stödfunktioner som finns och stödsystem och se till så att där finns en port.
IP3.90	J:	Och det tycker jag har varit jättebra gjort av om det är Margareta som tagit fram det eller inte, det har verkligen funnits en väldigt god service i det att den här informationsmaterial, de här PowerPoint presentationerna kring vad lagen innebär, vad är personuppgifter, allt det har framtagit redan och det fick vi till oss. Och det håller en helt annan kvalitet än om vi skulle sitta som inte jobbar med dem frågorna dagligdags att försöka sammanfatta och göra informationsmaterial om hur påverkar det här oss. Det tycker jag man har gjort jättebra, verkligen och också att även om vi är kontaktpersoner så har man ändå haft Margareta som kan de här frågorna mycket mera som har varit ute och informerat chefema, liksom gått ut så att det inte blir för mycket, så mycket faktakunskap som möjligt i detta.
IP3.91	I:	Finns det något sätt ni kan säkerställa att man når ut till alla som behöver veta?
IP3.92	J:	Via mail kan vi säkerställa det lätt, det kan man ju.
IP3.93	P:	Sen kan vi aldrig garantera att få något svar.
IP3.94	J:	Vi kan aldrig säkerställa att folk läser sina mail, men vi kan säkerställa att informationen går ut till alla, det kan vi.
IP3.95	I:	Om man tittar rent allmänt på informationssäkerhet är det någonting man jobbar med för att ha en medvetenhet om just informationssäkerhet i det dagliga arbetet?
IP3.96	J:	En som man gör, det man använder mest är våra journalsystem, där är alla medvetna om att man gör loggar av det, man tar stickprov varje månad för att se att man inte är inne i någons journal som man inte ska vara inne i. Jag tror det finns generellt.
IP3.97	P:	Det finns en struktur tänker jag som vi har, med både nån form av både samordnare på en nivå och ombud på enhetsnivå i väldigt många olika frågor, med regelbundna träffar och återkoppling. Det som kommer framförallt uppifrån som ska behöva nå ut går antingen i linje via cheferna eller i linje via ombud och samordnare. Verksamhetsområde har samordnare och enheter har ombud i en rad olika frågor där informationen behöver cirkulera egentligen både upp och ner. Ombuden samlar ihop sitt ifrån sina enheter och skickar vidare uppåt, det är tvåvägskommunikation på något sätt. Och det är så man hanterar de flesta så här större omfattande frågor, för att säkerställa att det finns och når ut på alla enheter. Ombudsfunktioner som finns framförallt brandombud, etikombud, barnombud you name it.
IP3.98	I:	Om man kommer som nyanställd har man någon form av information/utbildning för dem om hur man hanterar information i de olika systemen i organisationen, så de vet hur de ska göra på rätt sätt för att det ska bli så säkert som möjligt?
IP3.99	J:	Det ingår väl i introduktionen man har, dels är det som vanlig behandlare mest melior som är journalsystemet som är där du är inne och arbetar i och det är ju alltid en genomgång i och reglerna kring detta. Sen tror jag ju när det gäller andra system som vops till exempel det är det ganska många som är osäkra kring hur det fungerar och det är mest sekreterare som använder det.
IP3.100	P:	Jag tänker att alla nyanställda får ett introduktionsprogram på den enheten där dem kommer, som omfattar de här stora systemen också där man lägger mer eller mindre vikt vid en del saker, där finns ett paket som alla ska få gå igenom, till det kommer att verksamhetsområdet har introduktionsutbildning med föreläsningar ett tiotal ett par gånger om året som kommer med vissa jämna mellanrum där nyanställda uppmanas att gå på alla men det är öppet även för andra som känner att man kan välja ut nu behöver jag lite mer av detta, det är inte bara stora system utan även funktioner vi har inom vårt verksamhetsområde. ChÖL:ens roll, vad dem gör och vad vi kan använda dem till chefsöverläkare och

		lite annat sånt. Som är mer övergripande, sen tycker jag nånstans att det är upp till den enskilde medarbetarens egen ansvar att hålla sig uppdaterad vi har ju mycket information som når ut via nätet och vår egna utbildningsportal där vissa utbildningar är obligatoriska och som man då ser har du gjort den här, du har jobbat här ett par år och har fortfarande inte gjort den här utbildningen för det kan man dra fram, så får man sätta lite press på det. Sen finns det naturligtvis glidare överallt som lyckas tas sig igenom ändå, men det är ju ett chefsproblem nånstans, det är väl fördelen med att vara digitala, att man har hyfsad koll på vad folk är inne på, framförallt vad de inte är inne på som de borde vara inne på.
IP3.101	J:	Där Melior är liksom vårt största system.
IP3.102	I:	Har någon av er varit involverade i program/projekt som har haft med medvetandegörande av informationssäkerhet att göra, både inom Region Skåne eller någon annanstans?
IP3.103	J:	Jag har haft det i form av loggkontroll, jag är den som gör loggkontrollerna för vårt verksamhetsområde. Och då hade jag det att jag var ute mycket på enheterna och informerade om både vad det är som gäller liksom, när man får gå in i en journal och inte. Det tog nästan över ett tag att folk inte vågade gå in i några journaler alls och då blev det inte mycket jobb gjort. Utan var när är det man har rätt att gå in i journalerna, när har man inte rätt att göra det och hur fungerar det liksom. Nu tror jag nog det har satt sig.
IP3.104	P:	Jag har en tidigare Mina planer som är ett digitalt verktyg i den nya lagen om samverkan vid utskrivning i slutna hälso- och sjukvård, där jag tror jag varit ute på alla enheter, flera enheter mer än en gång för att informera och lite hands on om hur systemet fungerar och vad lagen säger, hur regelverket ser ut. Det har varit ganska omfattande och tar fortfarande mycket tid. man försöker fortfarande komma åt syftet, men det har inte riktigt satt sig plus att verktyget är lite trubbigt.
IP3.105	I:	Hur har det tagits emot just det här när du varit ute och?
IP3.106	P:	Det har tagits emot väl i den bemärkelsen att det har varit eftertraktat. Den pedagogiska svårigheten, eller det är mer specifikt Malmö men det är egentligen ett sidospår, två stadsdelar i Malmö vars jurister har förbjudit dem att använda systemet. Så Malmös 32 övriga kommuner använder systemet tillsammans med regionen. Vi har två stadsdelar, nej förvaltningar i Malmö och det dem vi har mest att göra med när det gäller fysiskt funktionshindrade vars jurister inte anser det vara nog säkert systemet för deras interna sekretess. Och det är en pedagogisk svårighet att tala om för dem att vi har ett hyfsat bra digitalt system som vi inte kan använda just när det gäller kommunikation med Malmö stad utan där får vi använda fax. Och i dessa tider är det en pedagogisk svårighet att få dem att se vitsen med lagen också hänvisar vi till faxen vilket innebär att på en normal patient som ska skrivas ut från slutenvården med den nya lagen innebär ungefär 22 stycken fax per patient det är dem enkla, är det komplicerade så är det uppemot 45–50 fax per patient. Det är ett helt annat sidospår. Men där är den verkliga utmaningen att försöka få dem att förstå lagen och syftet med den och sedan får jag hänvisa till att det inte går att använda det digitala verktyget fullt ut på grund av Malmö Stads jurister.
IP3.107	I:	Hur kompatibelt är det just framöver med GDPR?
IP3.108	P:	Anledningen till att det blir så många fax är att man hänvisar till säker faxrutin och säker faxrutin, då har du inga personuppgifter i faxen, så då klarar du dig i den bemärkelsen och sedan ska du skanna in materialet i din journal, men du ska ju först följa säker faxrutin först faxa en testsida, den ska du ringa upp och se så det finns en mottagare på andra sidan, så skickar du iväg faxet och sedan kompletterar du det med personuppgifter per telefon och sedan ska du få svarsfax från den andra att de har tagit emot det. Också varje gång du gör en ändring i denna plan, vilket ibland är ganska ofta, du har tre parter du har både slutenvård, öppenvård och kommun och ibland har du även primärvård och alla ska ha samma information. I IT-verktyget är det enkelt i den bemärkelsen att då skriver du din del i det här verktyget och sedan kan de andra se det och skriver sin del, men här ska du faxa runt en massa.

IP3.109	J:	Det känns ju jättesäkert också en massa lösa papper som figurerar.
IP3.110	P:	Nu har vi haft ganska stora påtryck på Malmö stad så nu har man hittat en teknisk lösning, fråga mig inte hur, som gör att dem ändå ska kunna, nu håller de på att testa denna. Så har jag tur så i månadsskiftet så köper dem den här lösningen och då kan vi fullt ut använda det fullt ut, men den kom i januari den här lagen och många fax har det blivit.
IP3.111	I:	Tycker ni det är något vi har missat att fråga om, något ni vill lägga till eller trycka mer på?
IP3.112	J:	Nej, mer att det känns som att det är tidigt, det är början liksom på detta arbetet nu och nu har vi gjort detta första steget.
IP3.113	P:	Jag tänker att den stora utmaningen ligger inte riktigt på vår nivå, utan man behöver skapa system som gör att vi kan efterleva lagen snarare än att lagen ska anpassa sig till oss. Där vi måste ha system där medarbetare ska kunna jobba som, de behöver ha de dokumenten de behöver för att jobba och göra ett bra jobb och då behöver någon skapa system som gör det så smidigt som möjligt, det ska vara lätt att göra rätt helt enkelt och där är kanske den stora utmaningen. Det är väl bra med den nya lagen säkrare för våra medborgare och patienter. Annars har ni fått med det mesta tror jag.
IP3.114	I:	Vi tackar för intervjun och överlämnar en liten gåva som tack för deltagande.

Appendix 5 – Intervju 4

Organisation: Beroendecentrum i Malmö och Trelleborg

Intervjuperson: Karina Stein

Yrkesroll: Områdeschef

Tid och plats: 10.30-11.30, torsdagen den 19 april 2018, personligt möte i Malmö

I: Intervjuare

K: Karina

Referens	Respondent	Frågor och svar
IP4.1	I:	Vi skulle gärna vilja att du börjar att berätta lite om dig själv och din roll här på arbetsplatsen.
IP4.2	K:	Ja ni vet vad jag heter, jag är områdeschef för Beroendecentrum och beroendecentrum är en del i vuxenpsykiatri i Malmö/ Trelleborg. Och fungerar ungefär som ett kompetenscenter för hela regionen. Vi är inte det formellt men vi hoppas kunna bli de ganska snart kring beroendepsykiatri, så vi är den enda specialiserade beroendepsykiatri inom region Skåne. Så jag har blandade verksamheter allt från beroende akutverksamhet, avdelningar för ineliggande vård och flera enheter i öppenvård för beroendevård och även spelberoende som är vårt senaste uppdrag. Mitt uppdrag är att jag är chef över cheferna, enheterna har en chef och jag är chef över dem. Jag är också chef över läkarna. Det innebär att jag försöker se till helheten, att helheten fungerar. Naturligtvis så är det alltid någon liten del som fungerar mindre bra. Då får jag lägga lite mer arbete där, men jag ser mitt huvudsakliga arbete att helheten ska fungera och mycket i samverkan med övrig psykiatri och framförallt socialtjänst och i viss mån kriminalvård också. Men vår största samarbetspartner är Malmö stad.
IP4.3	I:	Hur har förberedelserna inom Beroendecentrum sett ut inför att GDPR börjar gälla?
IP4.4	K:	Jag skulle vilja säga sett det är på två sätt vi har förberett oss. Dels så tycker jag nog ändå att jag ganska tidigt uppmärksammade att en lag skulle komma. Kanske lite av en händelse, jag är sambo med en jurist sedan många år men ett av mina barn hade också en rätt så avancerad uppgift i skolan kring personuppgiftslagen PUL där också GDPR kom in ganska tidigt. Så då började jag läsa på om GDPR och blev lite intresserad för att jag fattade att det var något nytt på gång. Sedan har jag tidigare också jobbat en del med kvalitetsregister psykiatriska kvalitetsregister. Där är PUL väldigt viktigt. Så jag tycker ändå att vi ganska tidigt inledde en dialog på beroendecentrum att detta är något som kommer att komma, man kan säga att det finns behov där vi inte ens uppfyller PUL. Sen har det ju skett ett centralt arbete som har kommit ganska mycket senare, som jag tycker påbörjades för en månad sedan kring städning av våra datorer i väntan på GDPR, där man också har påbörjat en inventering på hur ser våra behov ut, vi har en jätta massa listor och annat som inte kommer att uppfylla GDPR och hur behöver vi arbeta vidare med det. Så det finns en arbetsgrupp centralt och då inte på beroendecentrum utan på Region Skåne-nivå.
IP4.5	I:	Hur tycker du just att GDPR har påverkat dina arbetsuppgifter?
IP4.6	K:	Det har ju inte påverkat än för att vi är ju inte riktigt där, jag skulle säga att vi inte ännu är lagefterlevande men vi kan se att det kommer att påverka. Jag tycker såhär, att det som blir uppenbart när man jobbar med GDPR är att många av de datasystemen vi har inte är anpassade efter GDPR. Vi har ju två system vi arbetar med där personuppgifter som hanteras, dels är det ett som hanterar personal och de systemen är bättre tycker jag. Sedan har vi de som hanterat patienter och de är sämre, det handlar säkert om att när man har personal så har man de en och en. Men när vi har patienter på några av våra mottagningar så har vi 140

		besök på en dag. Då hanterar dessa systemen detta väldigt dåligt. För det är ju ungefär som, vid en och en person men när vi ska ha ett stort flöde, då fungerar dessa systemen väldigt dåligt. Där finns ju då extralistor som personalen ofta har på Excel och så, som vi inte får ha kvar då.
IP4.7	I:	Hur tror du då att förändringarna i arbetssättet kommer att bli?
IP4.8	K:	Det som är bra, tycker jag är att det har skapat en högre medvetenhet kring integritetsfrågor, alltså hur vi hanterar namn personuppgifter, i viss mån foto också. Så det tycker jag är bra, för den kunskapen kring hur vi hanterar detta, har varit lite dålig så det är det bra av det. Det som är dåligt då är ju lite klumpiga system. Där vi nog måste hitta nya system i de systemen som är godkända och som vi får använda.
IP4.9	I:	Det här med systemen är det något som ni kan påverka lokalt?
IP4.10	K:	Vi måste lyfta det. Alla de systemen är ofta upphandlade, det kan ju påverkas men vi måste föra fram informationen.
IP4.11	I:	Så du menar att just arbetssätten påverkas mer av systemen, och att man inte kommer kunna göra som man gör idag på grund av systemproblem?
IP4.12	K:	Man kan säga att vi har system som är ganska klumpiga och för att kunna arbeta i de systemen så måste man liksom ha listor och annat vid sidan om. Så vi skapar ad hoc lösningar. För att systemen inte uppfyller våra behov. Detta har vi ju återkopplat nu att detta måste lösas. Har man 140 patienter som man har på besök på tre timmar som vi har på vår helgmottagning. Då måste vi ha system som kan hantera det som är säkra. Och då har man ju haft mycket Excel listor för att det systemet som vi har som heter Vops inte hanterar det. Det är ju gjort för att patienterna ska komma en i taget och man lugnt ska kunna registrera patienten och så ser det ju inte ut i många verksamheter. Man måste också kunna ha det här överskådliga, har alla patienterna som skulle ha komma, kommit? Vi har ju patienter, så har de inte kommit så kan det ju ha hänt något väldigt illa. Det skulle ju egentligen, inte vara så svår tycker jag att få en lista på att nu har Kalle inte kommit, att vi lätt kunde se det. Men det kan vi inte i de systemen vi har.
IP4.13	I:	Vad tror du inom beroendecentrum vad kommer krävas för att ni ska kunna uppfylla kraven som GDPR ställer?
IP4.14	K:	Jag ser två vägar, det ena är att vi kan ha kvar våra listor, men hade på säkra e-platser. Precis som med säkra rum och stängda med lås, på datorn där vi kan förvara dem. Så säkra e-plaster är väl den ena lösningen, den andra är ju att det måste in men mycket mer funktionalitet i det systemen vi arbetar med. De är gammaldags, det är ju upphandlat ett nytt datajournalsystem till exempel, vårt datajournalsystem, Melior. Det är som en pappersjournal men där man har lagt den i datorn. Så ett mycket bättre system, mer funktionella system.
IP4.15	I:	Vet du om det nya systemet som är upphandlar uppfyller GDPR?
IP4.16	K:	Det hoppas jag i alla fall. Det tror jag för vi har haft ett annat system som heter SIP. Egentligen heter den utskrivningslagen. Tidigare hette den betalansvarslagen, nu heter den utskrivningslagen. Som började gälla den första januari i år. Har man en patient inlagd på en sluten vårdavdelning så ska det kallas till en SIP, samordnad individuell plan med kommunen. Då är det ett systemen som heter Mina Planer. Där har ju Malmö Stads jurister inte godkänt det på grund av GDPR så därför får vi hålla på att faxa till varandra istället. Så det tror jag med det nya journalsystemet har väldigt svårt att tro att det inte har varit med.
IP4.17	I:	Vad tror du blir den största förändringen i den dagliga verksamheten i och med GDPR?
IP4.18	K:	Det blir en omställningsperiod tänker jag när vi har blivit så pass medvetna om de listor och annat som vi har använt inte får användas. Så där är det ju att få in ett annan tänk. Det är ju en del av omställningsprocessen. Sen hoppas jag ju, vi

		måste ju komma till någon lösning. Antingen med säkra e-plaster eller bättre system. Men den mellanperioden innan vi är där. Kommer ju att bli lite svår för oss. Vi har ju börjat att rensa i listor då, ta bort personnumren till exempel eller bara ha ett förnamn för helt utan klara vi oss inte. Man har ändå ett behov, vad händer den här dagen? Som våra dagliga system inte kan ge oss. Som jag tycker att de borde kunna ge oss.
IP4.19	I:	Ser du att lagstiftningen berör vissa yrkesgrupper mer än andra? Och på vilket sätt i så fall?
IP4.20	K:	De som påverkas mest tror jag faktiskt är våra sjuksköterskor. För att det är dem som har det här snabba patientflödet och som måste ha en översikt, många patienter kommer under en dag. Jag är gammal psykolog och hade en patient i timmen så är de systemet vi har idag tillräckliga sådär påverkas jag inte så mycket, där behöver jag inte dra ut några listor. Så det är ju när man har stora patientvolymer på kort tid, snabba möten, det är ju de situationerna som påverkas mest.
IP4.21	I:	Vilka utmaningar tror du finns inom beroendecentrum?
IP4.22	K:	En utmaning är ju också att få personalen och i viss mån chefer att förstå vad en personuppgift är och det här integritetsskyddet alltså vikten av det. Det är en viss utmaning.
IP4.23	I:	På vilket sätt?
IP4.24	K:	Man har kanske varit så van att ha listor och jag brukar tänka så, hade jag velat detta? Om man till exempel jobbat på en avdelning med heroinberoende patienter kommer och där har man en lista över alla heroinberoende som ska komma den dagen, då brukar jag tänka så, hade jag velat ha mitt namn på en sådan lista? Men man skapar en form av, man får en referensram där det är helt okej att jobba på det sättet. Men det är det ju inte. Så ganska mycket handlar faktiskt om värderingar. Sen jag kan säga det att jag vet inte full ut hur GDPR fungerar utifrån det här med lagring av information. För det är ju också det här att man inte får spara information för länge. Till exempel journaler, polisen har ju reagerat på det till exempel med avlyssning och sådant. Telefonuppgifter och så, det kommer ju inte sparas så länge. <i>[en diskussion påbörjas där intervjupersonerna ger information till respondenten om hur GDPR fungerar i samband med journaler] [...]</i> . Sen är det ju ändå viktigt att vara striktare, vi har ju journalföringslagen som vi jobbar efter. Där brukar jag tänka som så, om jag har papper på mitt skrivbord, kanske något med patienten jag har gjort en bedömning eller gjort ett litet test, då får jag ju ha det som ett arbetsmaterial en kort stund sen ska det in i journalen. Eller så ska det kasseras. Där är det ju lite svårt ibland, så måste man ju hantera datamaterial också och få in det tänket, det är ju därför som vi håller på med den rensningen nu man kan ju inte spara på ett USB. Det kvittar ju egentligen om det finns på ett papper eller på ett USB Det ska liksom förstöras. Men det är att få in det tänket Det är ju inte så annorlunda i jämförelse med journalföringslagen egentligen.
IP4.25	I:	Tidigare om man tittar historiskt sett, har det skett någon större förändring som tidigare som har haft med information eller säkerhet eller informationssäkerhet att göra?
IP4.26	K:	Det har det väl, alltså PUL, kan man väl ändå säga, sen tycker jag inte fick samma genomslag men det är precis som vi har glömt bort PUL för att vi tycker att det är en sådan oerhörd stor förändring med GDPR, det är det ju egentligen inte. Utan den stora förändringen är ju egentligen att vi inte levt upp till PUL
IP4.27	I:	Hur hanterade man det när PUL kom? Gjorde man liknande genomgångar då?
IP4.28	K:	Nej. Inte mitt minne, jag jobbade i ett annat landsting, Västra Götaland. Men inte mitt minne att man gjorde det nej. Det finns ju PUL ombud och så, men det är lite dålig kunskap om att de finns. Det mesta jag har varit med om är just kvalitetsregister att patienter har velat radera sina uppgifter. Då måste man göra det. Det är mycket mer ljus på GDPR.

IP4.29	I:	Det du sa just med att radera från kvalitetsregister upplever du då att det har funnits något problem med det, som du säger att man inte har uppfyllt PUL, har man ändå haft koll på var allting är sparad?
IP4.30	K:	Nej, jag upplever nog att kvalitetsregistren hade man väldigt bra koll på det. De var ju godkända av PUL men problemet har ju säkert varit att man haft listor som man inte haft godkända av PUL. Att det har varit okej att, jag tänker på det här Rom-registret som polisen hade, kanske inte så stigmatiserande register men man kanske inte har förstått att har jag ett sådant register så måste jag ansöka om det till PUL. Det har man inte förstått rent allmänt. Några har ju naturligtvis förstått det, jag brukar säga så här, att, visst kan du ansöka till PUL om att upprätta det här registret men visst, lycka till. Du kommer ju aldrig att få ett ja.
IP4.31	I:	Om man då går vidare från GDPR, att medvetandegöra, hur går ni tillväga här på beroendecentrum för att informera medarbetarna om GDPR?
IP4.32	K:	Först har vi den här arbetsgruppen kring GDPR varit i vår ledningsgrupp och informerat alla chefer och alla chefer har fått i uppdrag att gå ut till alla medarbetare och säga att det ska börja städas, datorerna ska städas. Det skulle vara gjort innan den 15e april det var sista dagen för städning. Sen har cheferna också fått i uppdrag att inventera vilka behov de har för att vi ska kunna arbeta på ett effektivt sätt och ändå efter GDPR. Som det gör i sjukvården, det har gått i linje vi är ju en linjeorganisation
IP4.33	I:	Har man på något sätt sett till att alla medarbetare har blivit uppmärksammade?
IP4.34	K:	Ja, sen är det också så att dels är det ju chefsuppgifter att ta upp det med samtliga medarbetare, sen har det också gått ut mejl centralt till samtliga medarbetare att de ska städa sina datorer. Så det har varit både de vägarna, muntligt och via mejl. Sen vet vi ju att samtliga medarbetare inte läser sina mejl. Då tänker jag lite så, det kanske är lite slarvigt men, många av dem som inte läser sina mejl det är ju dem som inte jobbar så mycket med datorerna så är det ju faktiskt.
IP4.35	I:	Försöker man ändå som chef, säkerställa att man tar kontakt med de personerna?
IP4.36	K:	Det ska göras.
IP4.37	I:	Ni har inventerat och städat, vet du om det finns planer på att det ska komma nån mer utbildning för medarbetarna för att de ska bli medvetna om vad de behöver göra, hur de ska tänka för att följa GDPR?
IP4.38	K:	Nej det tror jag inte, utan den informationen har varit på chefsnivå. Chefer har erbjudits utbildning men inte till medarbetare. Vi har försökt här att jobba också, vi ar ett system som heter VOPS där man registrerar vårdåtgärder, och där har vi haft en arbetsgrupp också för att försöka få VOPS att funka, det får vi inte riktigt det är ett väldigt stelbent gammalt system känner man när man jobbar i det. Men där har ju också via det sprids kunskapen.
IP4.39	I:	Jag tänkte vad är det för typ av information som man har vidarebefordrat som chef till medarbetarna, vad är det man informerar om neråt?
IP4.40	K:	Dels är det den här städningen, sen har vi jobbat mycket på dom systemen vi har alltså att det är dem som ska användas, alltså inga listor vid sidan om, alltså rent hur man får det funktionellt i vardagen det har vi jobbat med.
IP4.41	I:	Om man då just ser när det gäller för att hålla personalen få dem medvetna om vad som gäller är det något som kommer arbetas med kontinuerligt eller är det att man får informationen en gång och sedan ska man kunna det?
IP4.42	K:	Jag hoppas ju att det blir något kontinuerligt annars får vi se till att det blir det. Det är en tendens att mycket blir precis som du säger man gör det en gång. För så tycker jag det har varit med PUL det är kanske ingen som riktigt brytt sig om PUL tyvärr, det var väldigt generaliserande, jag har brytt mig för PUL, att man måste jobba med det kontinuerligt. det är någonting ändå i samhället som är lite

		mer kring det har funnits kring datorer, ungefär som när det kommer ett nytt läkemedel man ser bara det positiva och nu börjar man se det negativa också. Och det som diskuteras jättemycket i sjukvården är digitaliseringen och då måste man ha in båda aspekterna av digitaliseringen både hur man kan använda det som ett hjälpmedel i vården men också hur det kan felanvänds. Så jag tänker att ändå är en stor diskussion, det är ju den digitaliserings diskussionen GDPR måste komma in också. Vi satt till exempel igår eller det finns ett beslut det största ledordet för Skånes sjukvårdspolitikerna det är tillgänglighet. Det står överst på agendan och sedan är digitalisering det är att minska sjukvårdens utgifter för att vi ska ha råd med välfärden det vill liksom digitaliseringen. De två sakerna måste liksom vävas in i varandra och då satt vi till exempel på ett möte igår och då finns ett beslut att patienterna innan årets slut skall sitta inne med sin egna legitimation och kunna gå rakt in i sjuksköterskors, läkares, psykologs tidböcker och boka besök. Så vi är mycket i e-lösningar och där måste GDPR in.
IP4.43	I:	Just det här med att göra det som en kontinuerlig process och göra medarbetarna medvetna om GDPR, anser du det är viktigt att medvetandegöra det?
IP4.44	K:	Absolut, jag tycker det är viktigt att få det som en del att man pratar inte bara GDPR utan man pratar digitalisering. Hur pratar vi liksom personuppgifter, integritet, hur systemen kan felanvändas att den diskussionen måste med i det.
IP4.45	I:	Hur gör ni då för att göra dem som jobbar i digitaliseringen och med systemen för att göra dem medvetna om att det är viktigt?
IP4.46	K:	Alltså jag tänker så här, nu har vi gjort lite här själva kring VOPS där vi har en arbetsgrupp och jobbar kring VOPS frågan för att få det till att lösas, sen är det ju också viktigt, ofta ser man saker i små delar och inom region Skåne jobbar man också med värdegrund och man måste få in det i värdegrundsarbetet, för mycket av GDPR det handlar naturligtvis om datorer och digitalisering men det handlar faktiskt också om värdegrund och personlig integritet. Och dom tänker i det värdegrundsarbetet som pågår, vi har tex etikombud, etikdagar jag tror faktiskt det är dem forumen det ska in
IP4.47	I:	Vad tänker du dig att beroendecentrum vill uppnå med just att medvetandegöra GDPR?
IP4.48	K:	För oss tänker jag så här, man har suttit tidigare och skrivit värdegrunder i verksamheter och jag har nästan alltid bara jobbat med tungt narkotikaberoende och då har jag tänkt så här att då blir det alla människors lika värde och då tänker jag nå, ja... räcker det när man jobbar med en heroinberoende kvinna som är prostituerad och misshandlad, asså räcker det att man säger att alla har lika värde är det tillräckligt? För oss är det också viktigt att veta att vi jobbar med en väldigt stigmatiserad grupp, det är inte okej att ha listor till exempel, vi har vår kvinnomottagning går man på den är man ofta prostituerad och heroinberoende, det är väldigt integritetskränkande och vi måste få in det i vårt tänkande, vi måste arbeta med dem frågorna. Därför är Det kanske extra viktigt när man jobbar med, det är viktigt överallt i samhället, men vi får inte glömma bort att vi jobbar med något som är väldigt stigmatiserande det får vi inte glömma bort.
IP4.49	I:	Tror du det krävs olika saker av enheter, om man jämför om man har en vanlig ortopedmottagning jämfört med era mottagningar?
IP4.50	K:	Jag tror att mycket av det kan vara lika, jag tror att sättet man kanske, vi får inte glömma bort att vi jobbar med stigmatiserade patienter, på något sätt ökar det kravet på oss. Kan bara ge ett exempel då vi har kanske i Malmö för att problematisera det 10 personer som är så farliga i Malmö att dem kanske inte kan behandlas på våra mottagningar för att vi inte kan garantera vår personals säkerhet, är det okej att ha dem på en lista, kan man skapa en sådan lista och ha dem på det, jag tycker inte det. Men där kanske inte alla tycker som jag, där tror jag kanske vi har ett annat problem än vad ortopederna har de kanske har en sådan lista för jättebesvärliga ortopedpatienter vad vet jag men jag tror inte det. Utan vi jobbar i en sfär där det ställs mer på sin spets, det tror jag faktiskt. Sen vet jag inte om jag är glasklar i det, jag tror vi har en annan utmaning faktiskt.

IP4.51	I:	Har du fått nån respons från dina medarbetare på dem här förändringarna i det dagliga arbetet eller överlag?
IP4.52	K:	Jag tycker vi har fått till en bra dialog, jag har hört att de flesta tänker för man gör saker av vana. När man sen börjar prata om det så tänker man liksom vad har vi hållit på med, att man faktiskt tycker det är bra. Vi är liksom väldigt vane styrda, man börjar på mottagningen och man har listor/det finns listor på allt i sjukvården och nej vi kan inte jobba med de här listorna vi måste hitta ett annat sätt att jobba, jag har inte märkt något negativt. Utan tröttheten är att vi har en del väldigt gammaldags system, där är väl tröttheten i det i så fall, men inte att någon inte tycker det är viktigt. Det tycker jag att alla tycker när man väl börjar prata om det.
IP4.53	I:	Och har ni inom verksamhetsområdet någon generell standard för hur man genomför förändringar som är stora policyförändringar liknande GDPR eller andra förändringar?
IP4.54	K:	Det har vi ju, man säga att vi följer mycket det som arbetsmiljölagen kring hur man gör stora förändringar som påverkar arbetsmiljön och medarbetarna, så det finns ett speciellt koncept kring hur man gör förändringar som vi jobbar med och det är att man risk och konsekvensanalyser, sedan gör man handlingsplaner efter dem. Nu går detta lite på tvärsen i och med att det är centralt på regionen också man har den här arbetsgruppen kring hur man arbetar med GDPR. Men jag tänker att förändringsarbetet som sker på enheten och som påverkar arbetsmiljön där finns där väldigt tydligt hur vi jobbar med det.
IP4.55	I:	Informationssäkerhet allmänt är det något ni jobbar med att medvetandegöra för medarbetarna i det dagliga arbetet?
IP4.56	K:	Ja, det tänker jag väl ändå det är något som diskuteras ganska mycket och det som diskuteras är både, jag har jobbat 20 år i VG region och jag tyckte vi hade tydliga rutiner i detta, till exempel vad händer om en patient mailar mig där var det förbjudet att maila tillbaka, då fick jag skriva ett brev eller ringa upp patienten. Det är lite mer flytande i region Skåne, det som är väldigt mycket diskuterat med kommunikationsavdelningen det är det här hur man använder sociala medier, vi har flera avvikelser faktiskt. Kanske inte att personal skriver om patienter men om andra medarbetare, chefen, verksamheten på ett väldigt utlämnande sätt på Facebook till exempel. Det finns till och med exempel där man har tagit foto på sin arbetsplats och lägger ut det på Facebook. Så det diskuteras mycket, det gör det.
IP4.57	I:	När de här situationerna kommer som du säger att mycket läggs ut på Facebook och sånt som inte borde om man säger av ren informationssäkerhet inte borde finnas där, hur gör ni för att informera medarbetarna och få in det i deras tanke-sätt?
IP4.58	K:	Där ligger väldigt mycket på enhetschefen, det är enhetschefen som är närmast medarbetaren. Både att prata om det på APT, men när man blir varse om att det skett så är det ett individuellt samtal som så, det kan till och med vara så att det handlar om ett sekretessbrott och då ska det faktiskt polisanmälas. Där kommer sekretesslagen också in.
IP4.59	I:	Och tidigare när du har jobbat både inom region Skåne och som du sa VG regionen, har du varit involverad i något projekt eller program som har haft med att man just ska medvetandegöra informationssäkerhet till medarbetarna?
IP4.60	K:	Det jag har varit med om, det är mer indirekt, vi har ett problem och hade också när jag jobbade i VG regionen det handlade mer om hot mot personal och där blanda vi in lite informationssäkerheten i det. Också utifrån hur man betar sig på sociala medier i det sammanhanget, vi vet ju och så är det i socialtjänsten också att har man socialsekreterare som till exempel omhändertar barn, det är en situation där vi också blir hotade med barn anmälan. Man kartlägger ofta människor via sociala medier och det är inte helt ovanligt att hot sker via sociala medier. Så där har jag varit med i Region Skåne hur man ska bete sig när man blir hotad, rutiner kring hot och våld och säkerhet, det har jag varit med och gjort upp, men

		där kommer informationssäkerheten med som en del av det och det är inte ovanligt att det sker den vägen.
IP4.61	I:	Hur gick man då tillväga för att göra medarbetarna medvetna om hur man ska jobba kring det här med hot och våld?
IP4.62	K:	Det är en linje i organisationen, det finns ett generellt sätt att jobba på det är samma sak i VG region och Region Skåne, dels är det att man ofta gör skriftliga rutiner som läggs ut på intranätet ofta i en säkerhetsportal eller kommunikatörsportal, HR-portal så att det är lätt och hitta för alla. Sen vet man ju att det är en väldigt liten del av medarbetarna som tittar där, men det är dem som gör det, det är bra att ha det samlat. Sen är det det här att det ska informeras på APT, det är enhetscheferna som har det största informationsansvaret.
IP4.63	I:	Är det något som även ligger, om man säger att det kommer nya medarbetare, som ligger med hur de ska bete sig rent allmänt när det gäller informationssäkerhet?
IP4.64	K:	Jag undrar, det är helt rätt det du säger det borde vara med i checklistan för nya medarbetare, men jag tror inte det är det, men du har helt rätt att det borde vara med. Det som diskuteras mycket på enheterna, det kanske är speciellt psykiatriin/beroendecentrum, det är säkerhetsproblematiken det är ofta återkommande diskussioner. Kring också att vi känner oss väldigt utlämnade.
IP4.65	I:	Har ni något speciellt då om man kommer som ny och inte har jobbat inom beroende tidigare för att hjälpa dem liksom att veta hur ska jag bete mig i olika situationer som kan uppkomma?
IP4.66	K:	Det finns speciell utbildning som alla medarbetare genomgår det heter Terma och där man också ska repetera varje år. Så det finns det, sen ska det också finnas handlingsplaner på varje enhet med lokala rutiner, men det finns en speciell utbildning, precis som vi har spiss som är suicidprevention, den ska också alla medarbetare genomgå och där man också noga kollar att alla gjort det.
IP4.67	I:	Är det någonting du tycker vi har missat att fråga, vill lägga till eller trycka mer på?
IP4.68	K:	Men jag tänker bara jag säger samma saker som jag har sagt tidigare lite. Man kan tänka GDPR väldigt smalt men jag vill gärna tänka GDPR brett och att jag tänker utifrån digitalisering, det kommer vi se mer av inom sjukvården hela samhället och det här värdegrundsarbetet som pågår, få in det, man måste tänka digitalisering värdegrund ihopa. Sen tror jag det har varit en lång period där vi bara har sett fördelarna med datorer och digitalisering, men att vi börjar se nackdelarna också och hur kan det här missbrukas
IP4.69	I:	Det du säger med värderingar, hur känner du att man kan implementera det på bästa sätt, att få personalen att anta värderingarna?
IP4.70	K:	Vi har värdegrundsspel, värdegrundsutbildning, så man jobbar ganska hårt på värdegrunden. Sen tänker jag att det viktiga när det gäller värdegrunden är ändå den kontinuerliga dialogen att man faktiskt tar upp det på APTerna, där man måste ställa sig frågan hur hade jag sett om mitt namn eller foto hade använts på detta sättet, man måste på något sätt sätta sig in i situationen. Men den där kontinuerliga dialogen är det viktiga, alltså vi vet att vi också är duktiga ibland på att man gör en jättestor insats sedan tappar man det är inget kostnadseffektivt sätt att arbeta. Ofta de här stora insatserna kan ha lite betydelse, ganska mycket slöseri med resurser egentligen, utan det är ju det här kontinuerliga arbetet.
IP4.71	I:	Vi tackar för intervjun och överlämnar en liten gåva som tack för deltagande.

Referenser

- Alfawaz, S., Nelson, K., & Mohannak, K. (2010). *Information security culture: a behaviour compliance conceptual framework*. Paper presented at the Proceedings of the Eighth Australasian Conference on Information Security-Volume 105.
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575. doi: DOI: 10.1016/j.chb.2015.03.054.
- AlHogail, A., & Mirza, A. (2014). *Information security culture: a definition and a literature review*. Paper presented at the Computer Applications and Information Systems (WCCAIS), 2014 World Congress on.
- Bryman, A., & Bell, E. (2017). *Företagsekonomiska forskningsmetoder* (2:2 ed.): Liber
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.
- Datainspektionen. (2018a). Artikel 4 Definitioner. Hämtad 2018-04-18, från <https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/>
- Datainspektionen. (2018b). Artikel 9 Behandling av särskilda kategorier av personuppgifter. Hämtad 2018-04-18, från <https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/>
- Datainspektionen. (2018c). Artikel 20 Rätt till dataportabilitet. Hämtad 2018-04-18, från <https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/>
- Datainspektionen. (2018d). Dataskyddsförordningen Förordningstexten i sin helhet. Hämtad 2018-04-17, från <https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/>
- Di. (2018). Relaterade ämnen och personer GDPR. Hämtad 2018-05-22, från <https://www.di.se/search?Query=gdpr>
- DN. (2018). GDPR. Hämtad 2018-05-22, från <https://www.dn.se/om/gdpr/>
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183.
- Frye, D. W. (2007). *Information Security Awareness Network Security Policies and Procedures* (ss. 179-193). Boston, MA: Springer US.
- Ghazvini, A., & Shukur, Z. (2017). *Review of information security guidelines for awareness training program in healthcare industry*. Paper presented at the Electrical Engineering and Informatics (ICEEI), 2017 6th International Conference on.

- Hassan, N. H., & Ismail, Z. (2016). INFORMATION SECURITY CULTURE IN HEALTHCARE INFORMATICS: A PRELIMINARY INVESTIGATION. *Journal of Theoretical & Applied Information Technology*, 88(2).
- Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. (2017). *Information security culture in health informatics environment: A qualitative approach*. Paper presented at the Research and Innovation in Information Systems (ICRIIS), 2017 International Conference on.
- Hayden, L. (2017). HIT HAPPENINGS. HOW TO ADOPT A SECURITY CULTURE. *For the Record (Great Valley Publishing Company, Inc.)*, 29(6), 30-31.
- He, Y., & Johnson, C. (2017). Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, 42(4), 393-408.
- HIMSS. (2017). *2017 HIMSS Cybersecurity Survey*. Hämtad från <http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf>.
- HLSF-FS 2016:40. *Socialstyrelsen föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården*. Stockholm: Socialstyrelsen
- ISO. (2013). ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls (ss. 80): International Organization for Standardization.
- Jacobsen, D. I. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen: Studentlitteratur*.
- Katsikas, S. K. (2000). Health care management and information systems security: awareness, training or education? *International journal of medical informatics*, 60(2), 129-135.
- Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., & Pestell, G. (2017). *Cyber security breaches survey*. University of Portsmouth.
- Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), 493-508.
- Ledendal, J. (2018). *Vägledning om dataskydd God integritet vid digital tjänste- och affärsutveckling (ss. 20)*.
- Malcolmson, J. (2009). *What is security culture? Does it differ in content from general organisational culture?* Paper presented at the 43rd Annual 2009 International Carnahan Conference on Security Technology.
- McIlwraith, A. (2016). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*: Routledge.
- Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health Information Security in Hospitals: the Application of Security Safeguards. *Acta Informatica Medica*, 24(1), 47.
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. *Journal of Systems and Information Technology*, 16(3), 210-221.

- MSB. (2015). *Uppföljning av informationssäkerhet i vården: Vårdgivarnas rapportering av kontroller, risker och incidenter*. Hämtad från <https://www.msb.se/RibData/Filer/pdf/27547.pdf>.
- OECD, O. f. E. C.-o. D. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*: OECD Publishing.
- Ramachandran, S., Rao, S. V., & Goles, T. (2008). *Information security cultures of four professions: a comparative study*. Paper presented at the Hawaii International Conference on System Sciences, Proceedings of the 41st Annual.
- Shoniregun, C. A., Dube, K., & Mtenzi, F. (2010). *Electronic healthcare information security* (Vol. 53): Springer Science & Business Media.
- Sujan, M. (2018). Managing health IT risks: reflections and recommendations. *Journal of Innovation in Health Informatics*, 25(1), 007-013.
- Sveriges Kommuner och Landsting. (2018). Förändringar för hälso- och sjukvården genom EU: s dataskyddsförordningen (förordningen) GDPR (ss. 8).
- TV4. (2018). Klipp och artiklar för ”gdpr”. Hämtad 2018-05-22, från <https://www.tv4.se/search?utf8=%E2%9C%93&q=gdpr>
- Wiles, J., Gudaitis, T., Jabbusch, J., Rogers, R., & Lowther, S. (2012). Chapter 8 - Information security awareness training: Your most valuable countermeasure to employee risk *Low Tech Hacking* (ss. 193-225). Boston: Syngress.