Examensarbete

HÖGSKOLAN I SKÖVDE

DATASKYDDSFÖRORDNINGEN GDPR:S PÅVERKAN PÅ BEFINTLIGA INFORMATIONSSYSTEM

En studie om hur befintliga informationsystem påverkas av GDPR, med fokus på Privacy by Design

THE GENERAL DATA PROTECTION REGULATION'S EFFECT ON EXISTING INFORMATION SYSTEMS

A study on the effect of GDPR on existing information systems, with focus on Privacy by Design

Examensarbete inom huvudområdet informationsteknologi med inriktning mot informationssystem
Grundnivå G2E 30 Högskolepoäng
IT607G, Vårtermin 2018

Hedwig Åkerman
a15hedak@student.his.se

Handledare: Marcus Nohlberg
Examinator: Rose-Mharie Åhlfeldt

Förord

Jag vill börja med att ge ett stort tack till det IT-konsultbolag som jag fått lov att utföra denna studie hos. De gav mig vägledning, uppmuntran och en trevlig arbetsmiljö vilket verkligen har uppskattats. Jag vill tacka samtliga intervjurespondenter i denna studie, som alla givmilt bidrog med tid och kunskap. Tack till de två anställda som deltagit i de observationer som har gjorts. Tack Rose-Mharie Åhlfeldt för detaljerad feedback som lett mig i rätt riktning.

Slutligen vill jag även ge ett stort tack till Marcus Nohlberg, min handledare, som har givit goda råd och utmanat med tankar kring hur studien bäst bedrivs, samt visat förståelse och vilja att hjälpa när jag känt mig fast eller vilsen på vägen.

- *Hedwig Åkerman*

Sammanfattning

Denna studie har undersökt hur den nya dataskyddsförordningen GDPR påverkar befintliga informationssystem. Genom arbetet har ett fokus även legat på metoden Privacy by Design och hur väl den uppfylls. GDPR ersätter Personuppgiftslagen i Sverige och innebär även att Missbruksregeln försvinner. Denna förändring kan tänkas resultera i större utmaningar för många företag, eftersom de krav som ställs är högre än tidigare. GDPR innebär ett utökat skydd för den personliga integriteten och ger EU:s medborgare fler rättigheter gällande hur personuppgifter bör behandlas.

I och med att många befintliga informationssystem ej skapats med hänsyn till mycket av det GDPR ställer krav på, finns en trolig risk att flera befintliga informationssystem blir svåra att uppdatera för att vara i linje med förordningen. Då GDPR även inkluderar krav med relevans till metoden Privacy by Design, är det troligt att företag som bättre uppfyller Privacy by Design även kan vara bättre i linje med GDPR. Från de deltagande respondenterna framgick det att en majoritet av de sju grundläggande principerna inom Privacy by Design uppfylls. Viss avsaknad kunde dock ses beroende på vilken organisation eller informationssystem det gällde.

Vad som ansågs mest utmanande med dataskyddsförordningen uttryckte samtliga respondenter var förståelse av innebörd och intention med förordningstexten. Gällande vad som upplevdes som det tekniskt mest utmanande kunde mönster identifieras för ett antal krav. De krav som identifierades som väsentliga för befintliga informationssystem att anpassas efter, samt vilka principer inom Privacy by Design som bättre uppfylldes, låg sedan i grund till en checklista. Checklistan blir ett redskap som ger en riktning för hur dessa punkter kan bemötas.

Nyckelord: Dataskyddsförordningen, General Data Protection Regulation, Privacy by Design, integritet, checklista

Abstract

This study has examined how the new data protection regulation GDPR affect existing information systems. The study has had a focus on the method Privacy by Design and how well its principles are fulfilled by different companies. In Sweden, the GDPR will replace the personal data act, 'Personuppgiftslagen'. This change may result in greater challenges for companies, since the requirements of GDPR are higher than they were before. The GDPR means a greater protection of privacy and it gives EU citizens more rights regarding how their personal data should be processed.

Many of the older, existing information systems weren't created with regards to what GDPR demands. It is possible that this creates a risk for several existing information systems not being compliant with the regulation, because of difficulties in updating the systems. The GDPR also includes requirements related to Privacy by Design, and it is likely that companies that better meet the Privacy by Design principles, are better compliant with the GDPR. From the participating respondents it was shown that a majority of the seven fundamental principles of Privacy by Design are met. However, an absence of some principles could be seen depending on the organisation or information system.

The most challenging aspect of the GDPR according to all respondents was to understand the meaning and intent of the regulation. Regarding what was perceived as the most challenging technical aspect of the GDPR, there were patterns for several requirements from the regulation. The requirements that were considered the essential ones for existing information systems to adapt to, as well as the principles that were better fulfilled were the factors the checklist was based on. The checklist can serve as a tool that provides a direction for how the identified issues can be addressed.

Keywords: General Data Protection Regulation, Privacy by Design, integrity, checklist

Innehållsförteckning

1 Inledning

I det västerländska samhället är de flesta människor idag uppkopplade på ett eller annat sätt. Antingen via mobiltelefoner, smarta klockor, smarta bilar, smarta hem med mera. Detta leder till enorma mängder av information som rör sig runt om i världen. En stor del av samhället består av individers profiler på sociala plattformar och i applikationer, där all möjlig information registreras. Bland denna information finns en hel del personuppgifter. När mycket av denna information är personlig blir det viktigt att den egna individen skyddas.

Den personliga informationen sparas i var och vartannat system som används i individers vardag. Det blir då centralt att ifrågasätta hur säker all denna personliga data är när den väl lagrats i ett informationssystem. Ökningen av behandling av personuppgifter är avsevärd och det kan tänkas att personuppgifter nu till och med har fått ett kommersiellt värde. Söktjänster och företag inom marknadsföring köper information i form av personuppgifter för att sedan kunna rikta reklam som är skräddarsydd efter personen i fråga. För att skydda data och information som lagras är en väsentlig faktor att tillämpa säkerhetsaspekter, särskilt på informationssystem som hanterar och lagrar personuppgifter. Genom ett fokus på att personuppgifter hålls säkra och behandlas på ett korrekt och tillåtet sätt, kan kränkning av individens personliga integritet undvikas. Informationssäkerhet kan ge systemägare förmågan att hos den information som lagras, bevara tillgänglighet, riktighet och konfidentialitet, samt spårbarhet, autenticitet, tillförlitlighet och oavvislighet (SIS-TR 50:2015).

I Sverige har informationssystem tidigare behövt följa Personuppgiftslagen (PuL) som har varit ett skydd av personuppgifter och medborgarnas integritet, genom att personuppgifter endast får behandlas i samtycke. Detta har givit Sveriges medborgare ett skydd mot att personuppgifter används mot någons vilja (Riksdagen, 1998). Detta kommer att ändras från och med den 25:e maj 2018, i och med att den nya dataskyddsförordningen General Data Protection Regulation (förkortat GDPR) träder i kraft. GDPR kommer därefter gälla som lag i samtliga av EU:s medlemsländer. Denna nya förordning innebär ett nytt och uppdaterat regelverk som ställer mycket högre krav på systemägare och verksamheter som hanterar personuppgifter. GDPR lyser ljus på och sätter den personliga integriteten och skyddet av medborgarnas information först med målet att skydda EU:s medborgare från brott där deras personliga data utnyttjas. GDPR skulle kunna beskrivas som en utökning av PuL med ett ytterligare skydd av medborgarnas personliga information, eftersom mycket av det som finns inom PuL även återfinns inom GDPR (Datainspektionen, 2017a). GDPR blir en vändpunkt för datasekretess och integritet inom företag i EU och kommer ge användare mer kontroll över de personuppgifter de lämnar ifrån sig.

Många organisationer och verksamheter kommer troligtvis påverkas till stor grad av de nya kraven som kommer med GDPR. Detta i och med att kraven är mycket omfattande och kan ha en stor påverkan på de informationssystem som används.

Inom GDPR finns även krav baserade på principer inom metoden Privacy by Design (PbD). De krav som kommer med Privacy by Design (PbD) uppmanar systemägare och systemutvecklare att implementera tekniska och organisatoriska åtgärder, samt dataskyddsprinciper till organisation och system (Europaparlamentets och rådets förordning (EU) 2016/679). Bemötandet av dessa krav kan göras genom att organisationer tillämpar informationssäkerhet. Genom att använda informationssäkerhet kan de skydda information som organisationer och verksamheter hanterar i sina system. Att därmed även se över principerna inom Privacy by Design kan det leda till att organisationer får tydligare informationssäkerhet och samtidigt går i linje med GDPR.

Inför att den nya förordningen träder i kraft är det tänkbart att organisationer vill veta om de system de använder är korrekt utrustade. Samtidigt kan det även underlätta att kunna avgöra om framtida utveckling av system också går enligt GDPRs krav. Det blir därmed av intresse för organisationer och verksamheter att veta hur deras befintliga informationssystem kan behöva uppdateras för att vara i linje med GDPR.

Genom att utforma en checklista som ställer frågor utefter GDPR och Privacy by Designs krav, kan befintliga system ses över för att avgöra hur redo de är. Checklistan blir ett medel för systemägare att få en tydlig bild över om någon del av ett system behöver åtgärdas och uppdateras. Vidare kan checklistan även ge riktlinjer för vilken typ av ingripande och åtgärd som kan behövas. Tillämpning av en checklista kan tänkas bli en påminnelse av vad som bör implementeras i informationssystem och organisation. Därmed kan en checklista bli en bidragande hjälp att hålla ett konsekvent arbete som är i linje med GDPR.

2 Bakgrund

Detta kapitel ger information om bakomliggande begrepp som är av vikt i studien. Kapitlet ger en förståelse för det skydd den nya dataskyddsförordningen GDPR kommer ge, samt dess koppling till informationssystem och säkrandet av personers integritet. Kapitlet förklarar även innebörden av metoden Privacy by Design.

2.1 Informationssystem

"Med ett system menar vi en mängd komponenter som är förenade till en helhet."
(Gustafsson, et al., 2009, p. 16)

Varje komponent inom ett system har yttre egenskaper som i sin tur påverkar de andra komponenterna. Samtliga komponenter bildar tillsammans en helhet. Helheten får därmed egenskaper som vanligtvis inte kan återfinnas i en enskild komponent. Istället blir dessa egenskaper synliga i strukturen när komponenterna existerar tillsammans. Begreppet system kan alltså ses som ett generellt begrepp då det kan användas för att representera flera olika helheter inom olika områden (Gustafsson, et al., 2009).

En liknande beskrivning av hur ett system kan definieras görs av Bocij, Greasley och Hickie (2015), där de beskriver ett system som en samling komponenter som tillsammans arbetar efter samma mål. Systemets funktion är att ta emot 'input' för att sedan omvandla detta till 'output'. Det mål som systemet arbetar efter kan oftast beskrivas kort och koncist med endast någon enstaka mening. Det är ovanligt att system är isolerade, istället brukar det finnas en omgivning kring systemen som innehåller antingen andra system eller externa organ. Systemet har ett omfång och detta omfång kallas för *scope*. Ett systems *scope* definieras av dess avgränsning där allt inom avgränsningen är del av systemet självt (Bocij, et al., 2015).

Informationssystem brukar vanligtvis inkludera datorer där de tillsammans möjliggör för verksamheter att utföra sin affärsverksamhet på nya och förändrade sätt. Ett exempel är grossister och affärer som samlar in data från sina olika butiker. På så vis kan de anpassa påfyllnaden av lagervaror till sådant som kunderna vill ha och därmed reducera sina kostnader (Stair, Reynolds och Chesney, 2008). Både organisationer och personer använder information dagligen; vi har tillgång till mängder med information över Internet och vi får tillgång till information via exempelvis tidtavlor på busshållplatser och centralstationer m.m.

Stair, Reynolds och Chesney (2008) förklarar hur komponenterna inom ett system samlar in, lagrar, manipulerar och sprider information för att sedan tillhandahålla en form av feedback-mekanism. Det är denna feedback som möjliggör för organisationer att nå sina mål, såsom till exempel ökade intäkter eller reducerade kostnader. Feedback är den information som systemet ger tillbaka till organisationen. Denna information kan användas för att genomföra förändringar av input- eller bearbetning (Stair, et al., 2008).

Dessa datorbaserade system beskriver Stair, et al., (2008) att de har en allt ökad användning för att lagra, skapa och förflytta information. Informationssystem gör att tillverkare och producenter av produkter kan både beställa och distribuera sina varor snabbare än vad de någonsin kunnat tidigare. Information finns i många olika former, till exempel text, bilder, siffror, eller ljud- och videofiler, men det är inte helt ovanligt att begreppet information förväxlas med begreppet data. Båda dessa begrepp är nära relaterade, men de kan särskiljas genom att data är den input som ges till ett system. Efter att denna data har bearbetats i informationssystemet, ges output i form av information (Stair, et al., 2008).

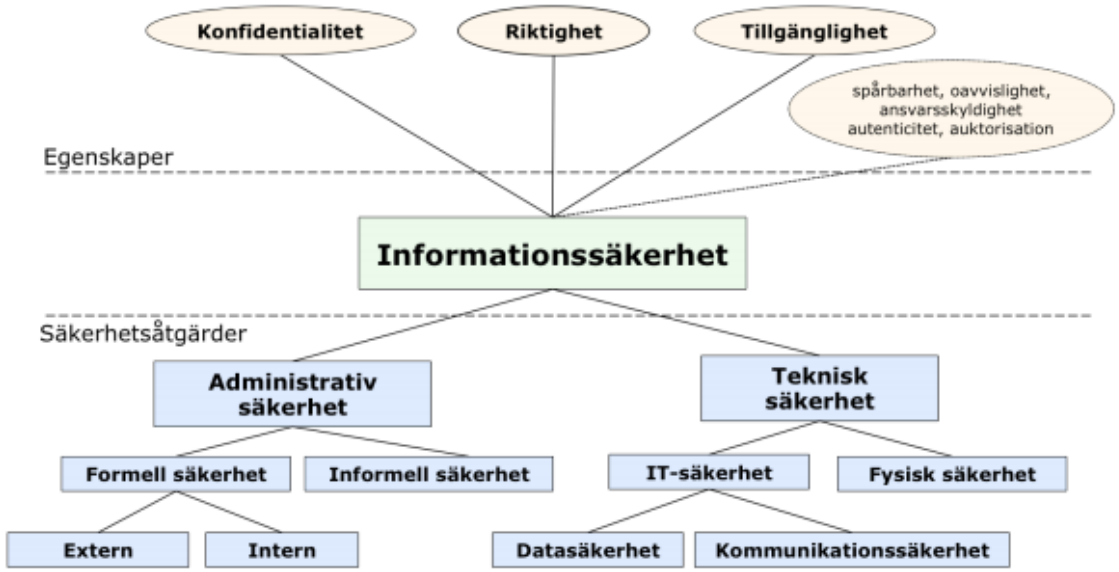
2.2 Informationssäkerhet

Den teknologiska utvecklingen kan tänkas ha lett till mer avancerade och bättre utrustade cyberbrottslingar. Enligt Campbell (2016) är kapaciteten mycket högre hos cyberbrottslingar nu än den tidigare varit, men de är även mer sofistikerade. De har blivit till hotfulla aktörer som genom teknisk överlägsenhet undersöker och utvecklar lömska skadeprogram. Dessa program tillåter dem att ta sig in i och få tillgång till system samtidigt som de täcker sina spår. Författaren fortsätter med att säga att cyberbrottslingarna idag även har en mycket mer robust inställning till informationssäkerhet än vad många legitima företag har. Detta gör det svårare för polisen att försöka bekämpa dessa nätverk av cyberbrottslingar, då det också blir svårare att upptäcka dem (Campbell, 2016). Det är troligt att samma sak kan gälla för olika organisationer och verksamheter, som även de behöver arbeta extra mycket för att försöka säkra sig från denna typ av kriminalitet och cyberbrott. Det blir då viktigt att organisationer och verksamheter genomgående arbetar med informationssäkerhet för att säkra både system och information, men även för att säkra arbetsplatsen i sig. Uppmärksammandet av säkerhet som kommer med GDPR kan troligt ge upphov till utökad informationssäkerhet inom organisationer, vilket går hand i hand med förberedelse för att uppfylla lagens krav.

I Swedish Standards Institute (förkortat SIS) standard SS-EN ISO/IEC 27002:2017 som *”ger vägledning för organisationers interna normer för informationssäkerhet och praktisk hantering av informationssäkerhet”* (SS-EN ISO/IEC 27002:2017)*,* beskrivs informationssäkerhet som en förmåga att kunna bevara konfidentialitet, riktighet och tillgänglighet hos information. Vidare kan begreppet informationssäkerhet också innebära närvaron av spårbarhet, tillförlitlighet, oavvislighet och autenticitet (SIS-TR 50:2015).

Ett tillvägagångssätt för organisationer att arbeta med informationssäkerhet är att bruka ett holistiskt perspektiv. Detta inkluderar både teknisk säkerhet och administrativ säkerhet i säkerhetsarbetet. Genom att arbeta med bägge delar kan dessa komplettera varandra och organisationen kan på så vis täcka ett större område och ha en mer genomgående informationssäkerhet inom organisationen. Kompletteringen av båda typerna av säkerhet kan även leda till att organisationens information bättre kan

uppfylla tidigare nämna begrepp inom informationssäkerhet. Se Figur 1 nedan för en illustration av uppbyggnaden av informationssäkerhet.



Figur 1 ***Informationssäkerhetsmodellen*** *(Åhlfeldt m.fl., 2007; SIS, 2015, pp 73-84)*

2.3 Personuppgifter

Personuppgifter täcker en hel del olika typer av information och det kan antas att inte alla dessa olika typer är självklara personuppgifter. En personuppgift är något som direkt eller indirekt kan hänvisa till en fysisk person. Det vill säga, all information som kan identifiera eller knytas till en riktig person som är i livet. De personuppgifter som direkt kan kopplas till en fysisk person är exempelvis personnummer och namn. Indirekta personuppgifter kräver ytterligare information för att identifieringen ska kunna ske. Exempel på denna typ av personuppgifter är registreringsnumret till ett fordon, IP-adresser eller e-postadresser (Personuppgiftslag (1998:204), 2018).

I den nya dataskyddsfördordningen GDPR ges en egen, mer utvecklad definition av innebörden av personuppgifter,

"...all information som är relaterad till en identifierbar eller identifierad person; en identifierbar, fysisk person är någon som kan bli identifierad, direkt eller indirekt, speciellt via referens till en identifierare såsom ett namn, ett personnummer, data över geografisk position, en online-identifierare eller en eller flera faktorer som är specifika till den fysiska, psykologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identiteten hos den fysiska personen;" (Europaparlamentets och rådets förordning (EU) 2016/679, p. 33)

2.4 General Data Protection Regulation (GDPR)

I april 2016 godkände EU-parlamentet den nya dataskyddsförordningen General Data Protection Regulation (GDPR) efter att diskussion och debatt hade pågått i fyra år (EU GDPR, u.d.). Denna nya dataskyddsförordning kommer träda i kraft den 25e maj 2018 och kommer gälla som lag för alla länder inom EU. Detta innebär även att den kommer att ersätta vissa nationella regler, såsom Personuppgiftslagen (PuL) i Sverige. Från det att GDPR börjar gälla, ersätts därmed även det tidigare direktivet 95/46/EG.

År 1995 startades direktivet, 95/46/EG för att skydda personuppgifter och det är detta direktiv som därefter gällt inom EU. Eftersom vår vardag ser annorlunda ut idag, går det tidigare direktivet inte längre helt i linje med en värld där mycket är data- och teknikdrivet. Nyckelprinciperna i direktivet från ’95 är fortfarande sanna och appliceringsbara, men med GDPR kommer fler, nya regler och reglerande policys. Dessa nya riktlinjer kommer påverka hur verksamheter och organisationer får lov att lagra och hantera personliga data (Europaparlamentets och rådets förordning (EU) 2016/679).

För alla som hanterar personuppgifter är det kritiskt att GDPR följs. Alla företag eller andra organisationer och myndigheter måste visa att de aktivt tar ansvar för att följa GDPR. Skulle en överträdelse av GDPRs ske, utdöms en sanktionsavgift. Beroende på hur allvarligt fallet är, avgörs avgiften därefter. För att avgöra allvarlighetsgraden tittas det på om överträdelsen skett avsiktligt, om det har lett till en ekonomisk vinst för de som begått överträdelsen, vilka åtgärder som vidtagits, samt andra omständigheter som på något vis kan ha varit förmildrande eller försvårande för fallet i fråga (Europaparlamentets och rådets förordning (EU) 2016/679) (Datainspektionen, 2017b).

Till följd av GDPR tillkommer flertal nya regler för hur personuppgifter får lov att behandlas. Flera punkter inom förordningen har likhet med de regler som idag redan finns i Personuppgiftslagen i Sverige. Exempelvis att personuppgifter endast får behandlas i samtycke från personen vars uppgifter det handlar om. Krav som tillkommer med den nya dataskyddsförordningen och som skiljer sig från PuL beskrivs i följande delkapitel nedan.

GDPR medför att uppgifterna måste skyddas på rätt sätt och tillräckliga säkerhetsåtgärder måste finnas på plats där uppgifterna lagras. För de uppgifter som berör etniskt ursprung, hälsa, religion eller politisk uppfattning ställs även särskilda krav (Datainspektionen, 2017b). I kapitel 1, Artikel 1 i dataskyddsförordningen GDPR ges följande beskrivning av förordningens innebörd,

”1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.

2.Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter."
(Datainspektionen, 2017g)

Tikkinen-Piri, Rohunen och Markkula (2018) från Universitet i Oulu, Finland, undersökte vilka nya utmaningar GDPR medför för organisationer som behandlar personuppgifter kontra direktivet från 1995. Författarna identifierade tolv aspekter som ansågs mest kritiska att ta hänsyn till. Dessa aspekter var följande:

1. Specificering av syfte och omfattning av behandling av data
2. Ta hänsyn till villkor för internationell databehandling
3. Skapa integritet genom inbyggt dataskydd och dataskydd som standard
4. Påvisa att GDPR krav följs genom förhållningspolicy ('codes of conduct')
5. Skapa processer som hanterar dataintrång
6. Beräkna sanktionsavgift för att ej fullständigt följt förordningen
7. Utse ett Dataskyddsombud (om applicerbart)
8. Förse individer med information om behandling av personuppgifter
9. Erhålla samtycke om behandling av personuppgifter
10. Möjliggöra för 'Rätten att bli glömd'
11. Möjliggöra för Dataportabilitet
12. Upprätthålla dokumentation

(Författarens egna översättning från engelska) (Tikkinen-Piri, Rohunen & Markkula, 2018, p. 147)

Författarna lyfte att alla företag som bedriver någon form av övervakning av EU-medborgares beteende eller som hanterar EU-medborgares personuppgifter bör se över befintliga tekniska och organisatoriska skyddsåtgärder gällande integritet. De påpekade även att dessa företag eventuellt också bör utveckla sina befintliga principer med nya åtgärder som går i linje med GDPR. Författarna menade att de tolv identifierade aspekterna är relevanta för att följa förordningen i företag med personuppgiftsdata (Tikkinen-Piri, Rohunen & Markkula, 2018).

2.5 Privacy by Design

Privacy by Design (PbD) är en metod skapad av Dr. Ann Cavoukian, känd som en av de främsta experterna inom integritetsfrågor. Dr. Cavoukian var tidigare ledamot för information och integritet för provinsen Ontario i Kanada under hela tre mandatperioder och det var under hennes tid som ledamot som hon skapade Privacy by Design (Keoshkerian, u.d).

Innebörden av metoden är att fokus och åtanke alltid hålls för säkerheten av personers privata information. Detta ska ske under hela utvecklingsprocessen av system, annan teknik, operativa system, fysiska utrymmen, nätverksinfrastruktur och arbetsprocesser. Privacy by Design anbefaller att integritet byggs in direkt i design och utformning, samt i arbetsprocessen av utvecklingen. Cavoukian (2010) uttrycker att omfattningen för PbD sträcker sig till tre primära applikationer nämligen (1) IT-system, (2) ansvarskrävande affärspraxis och (3) fysisk design, samt nätverksinfrastruktur (Cavoukian, 2010).

Privacy by Design beskrivs av Dr. Cavoukian med sju grundläggande principer och vid implementation av metoden krävs det att dessa uppfylls. De sju principerna är följande,

Proactive not Reactive; Preventative not Remedial

Denna princip beskriver ett av kännetecknen för PbD, nämligen proaktivitet. Åtgärderna inom Privacy by Design är proaktiva snarare än reaktiva, då de förutser och förhindrar att något inträffar som bryter integriteten. Syftet med metoden är att hindra överträdelser från att uppstå. PbD väntar därför inte på att risker ska bli till verkliga hot och har inte något fokus på att erbjuda lösningar när något har inträffat - metoden förhindrar istället att riskerna kan bli till allvar från första början (Cavoukian, 2010).

Privacy as the Default

Privacy by Design vill leverera den högsta graden sekretess och integritetsskydd genom att personuppgifter automatiskt ska skyddas genom exempelvis ett givet IT-system, genom affärspraxis eller affärsprinciper och rutiner; genom implementerade standardregler inom verksamheten. Ingen åtgärd ska behövas göras av en individ för att skydda sin integritet, detta ska vara inbyggt som standard i systemet; om handling inte krävs av en individ hålls integriteten därmed orörd (Cavoukian, 2010).

Privacy Embedded into Design

Integritetaspekten ska inte komma som ett tillägg och något som kommer i efterhand efter att ett system är färdigbyggt. Integriteten ska vara inbäddad redan från start i design och i arkitekturen för systemet eller affärsmetoderna. När ett system eller en metod levereras blir integritet därmed en av de grundläggande funktionerna och en essentiell del då det är integrerat i själva systemet (Cavoukian, 2010).

Full Functionality—Positive-Sum, not Zero-Sum

Privacy by Design vill visa hur det är möjligt att ha både integritet och säkerhet samtidigt och skapa en balans där inga kompromisser för något av begreppen sker - en win-win situation. Ofta infinns ’zero-sum’ som tillvägagångssätt inom organisationer, vilket innebär ”antingen-eller”; ofta sker val mellan antingen integritet *eller* säkerhet,

integritet *eller* affärsintressen. Genom att avvisa 'zero-sum' för att istället använda 'positive-sum' kan två positiva ökningar i två olika områden finnas samtidigt. Integritet och affärsintressen eller säkerhet flätas samman och ökar tillsammans. När samtliga begrepp erhålls och är positiva kan kompromisserna undvikas och en balans uppnås. (Cavoukian, 2010).

End-to-End Lifecycle Protection

Den inbäddade integriteten i system ska sträcka sig hela vägen från start till slut. Det vill säga att integriteten finns under hela livscykeln av den data det berör. Innan den allra första informationen har samlats in, finns integriteten redan inbäddad i systemet. Detta medför att vid slutet av livscykeln kommer data att i tid raderas på ett säkert sätt när exempelvis ett IT-system tas ur bruk (Cavoukian, 2010).

Visibility and Transparency

Privacy by Design har som mål att försäkra samtliga intressenter att oavsett vilken affärspraxis eller affärsprinciper och teknologi som är inblandad, verkar de på ett sådant sätt som är i enlighet med de mål och löften som har ställts upp. Komponenter och funktioner ska förbli synliga för både leverantörer och användare; det ska finnas förtroende men viss granskning måste ändå genomföras (Cavoukian, 2010).

Respect for User Privacy

Det främsta kravet som Privacy by Design ställer på arkitekter och på operatörer av system, är att erbjuda åtgärder såsom lämpligt beaktande, användarvänliga alternativ, samt starka standardvärden för integritet. Detta för att hålla intresset för individens säkerhet i första hand (Cavoukian, 2010)

2.6 Privacy by Design inom GDPR

Inom GDPR ställs det krav baserade på Privacy by Design. Dessa formuleras i Artikel 25 i förordningen som "Data protection by Design and by Default" eller "Inbyggt dataskydd och dataskydd som standard" på svenska. I tillägg till denna artikel finns 'Skäl 78' som är en uppräkning av de åtgärder som förväntas göras för att bemöta kraven inom Artikel 25. Åtgärderna som exemplifieras inom Skäl 78 är dataminimering, att pseudonymisera data så snart som möjligt, att göra det möjligt för personer vars data behandlas att få information om behandlingsprocessen; att vara transparent med funktioner och behandling av personliga data, med mera. Det uppmuntras även att sätta nya policys i bruk och implementera åtgärder som bemöter principerna för detta krav. I GDPR definieras Privacy by Design enligt följande,

"Med hänsyn till den tekniska utvecklingsnivån, kostnaden för genomförandet och behandlingens art, omfattning, sammanhang och ändamålet med behandlingen, samt riskerna för varierande sannolikhetsgrad och allvar för rättigheter och friheter för fysiska personer som orsakas av behandlingen, ska personuppgiftsansvarig person ta till tekniska och organisatoriska åtgärder, som är utformade för att implementera dataskyddsprinciper, för att på ett effektivt sätt integrera nödvändiga skydd i utvecklingen…" (Europaparlamentets och rådets förordning (EU) 2016/679, p. 15).

De krav som ställs i Artikel 25 innebär att den individ som är personuppgiftsansvarig förväntas implementera lämpliga åtgärder, både inom teknik och organisation. Detta för att på ett effektivt sätt, inkludera dataskyddsprinciper i sina system och i sin organisation. Dessa dataskyddsprinciper fungerar som åtgärder för att säkerställa att det som standard endast är personliga data som är helt nödvändig, för varje specifikt ändamål av behandlingen av data, som behandlas. Denna skyldighet hos verksamheterna gäller för mängden personuppgifter som samlas in, tiden för hur länge de lagras, samt omfattningen av behandlingen och tillgängligheten av uppgifterna. Åtgärderna ska också säkerställa att personuppgifter inte görs tillgängliga utan individens egna ingripande. Detta ska även inkluderas som en standard inom organisationer. Principerna blir även ett sätt att integrera nödvändiga skyddsåtgärder i bearbetning och behandling av data. Som tidigare nämnt, är exempel på sådan teknik som uppmuntras i förordningen är pseudonymisering och dataminimering. Åtgärder som dessa kan bidra till att förordningens krav uppfylls och de registrerades rättigheter kan skyddas (Europaparlamentets och rådets förordning (EU) 2016/679). De krav som ställs inom Artikel 25 känns igen inom metoden Privacy by Design. Det kan därmed antas att det kan vara enklare för en organisation att vara i linje med GDPR genom att ha grundprinciperna inom Privacy by Design implementerade inom verksamheten.

Förordningen uppmuntrar systemägare och utvecklare att ta hänsyn till rätten till dataskydd och kontrollera att registreringsansvariga och registerförare kan fullgöra de skyldigheter de har. Dessa skyldigheter är att skydda data även vid nyutveckling, utformning och användning av tjänster, applikationer och produkter som bygger på behandling av personuppgifter. Inom ramen för offentliga upphandlingar bör principerna för dataskydd av design och standard också beaktas (Europaparlamentets och rådets förordning (EU) 2016/679).

2.6.1 Pseudonymisering

"behandling av personliga data på ett sådant sätt att denna data inte längre kan hänföras till ett specifikt data-subjekt utan användning av ytterligare information."
(Europaparlamentets och rådets förordning (EU) 2016/679, p.33).

Pseudonymisering innebär att data separeras från de direkta identifieringstecknen, vilket medför att länkningen till en identitet inte längre är möjlig om inte ytterligare information som finns separat, erhålls. De fält som är som mest identifierande inom ett dataset ersätts istället med ”artificiella identifierare” eller pseudonymer. Detta är något som kan minska risker i samband med databehandling avsevärt, samtidigt som användbarhet hos data bibehålls. I och med detta skapar GDPR motiv för varför systemägare bör använda pseudonymisering av den data de samlar in. Pseudonymiserad data är inte undantagen de resterande krav som GDPR ställer, men förordningen släpper efter an aning på några krav för de systemägare som använder sig av tekniken (Europaparlamentets och rådets förordning (EU) 2016/679).

Pseudonymisering av ett dataset sker genom att all övrig information hålls separat. Denna information måste säkerställas att den inte hänförs till en identifierbar eller identifierad person och ska därför omfattas av organisatoriska och tekniska åtgärder. När identifieringstecknen ersätts av pseudonymer eller ”artificiella identifierare”, leder det till att kopplingen inte längre kan göras utan den övriga, identifierande informationen. Det är alltså en teknik för att förstärka säkerheten av integriteten där direkt-identifierande data hålls säkert och separat från den data som har behandlats. Det är angeläget att poängtera hur GDPR fastställer i Skäl 28 att pseudonymisering *”inte är avsett för att utesluta alla andra åtgärder för dataskydd”* (Europaparlamentets och rådets förordning (EU) 2016/679, p. 5).

2.6.2 Dataminimering

Innebörden av dataminimering är att den information som samlas in ska vara relevant och lämplig, samt nödvändig för syftet bakom själva behandlingen av data. Mer data än det som krävs för syftet av insamlingen ska varken lagras eller behandlas, vilket även minimerar hur mycket data det är som finns tillgänglig och kan härledas till en identifierbar person (Europaparlamentets och rådets förordning (EU) 2016/679).

2.7 Ostrukturerad och strukturerad data

Strukturerad data är data som är mycket organiserad och lätt att behandla. Detta medför att analys blir möjligt att genomföra med legacy-lösningar inom data mining. Innehållet av strukturerad data är till största del kunddata, såsom adresser, namn och kontaktinformation. Denna typ av data består till största del av textfiler där informationen är väl-organiserad. Data lagras sedan i ett data warehouse varifrån den kan hämtas för analys. Strukturerad data är alltså till största del system för ärende- och dokumenthantering, databaser och traditionella dataregister (King, 2017).

Ostrukturerad data består istället till största del av strömmad data från exempelvis mobila applikationer och sociala medier-plattformar, positionstjänster och Internet of Things-teknologier. Exempel på detta skulle kunna vara e-post, information från webbplatser eller ljud- och bildupptagningar. Rådande inom just ostrukturerad data är den mångfald som finns. Detta leder till att företag kan få det svårare att behandla denna typ av data, än vad de tidigare haft med enbart strukturerad data. Till skillnad från strukturerad data kan inte ostrukturerad data lagras i ett Excel-spreadsheet eller i en datatabell, utan istället kräver denna typ av data specialiserade förmågor och verktyg. Traditionella data warehouse-miljöer passar därför inte denna typ av data (King, 2017) (Taylor, 2017)

Missbruksregeln

I och med att GDPR träder i kraft kommer vad som kallas för ”‘Missbruksregeln’” att försvinna. Missbruksregeln innebär enklare regler för de personuppgifter som är ostrukturerade. Att missbruksregeln inte kommer finnas kvar innebär att det är samma regler som kommer gälla både för strukturerade och ostrukturerade personuppgifter (Datainspektionen, 2017c). Hanteringen av personuppgifter på webbplatser, i e-post

m.m. ska vara densamma som för personuppgifter som är lagrade i databaser eller andra hanteringssystem. Detta betyder att en rättslig grund måste finnas och information ska ges till de registrerade. Det ska även föras register över behandlingarna som görs. När det gäller personuppgifter som skickas via e-post eller vid webbpublicering av personuppgifter, bör en organisation se till att rutiner och instruktioner gällande detta är tydliga nog, eller om de behöver ändras eller kompletteras för att uppfylla GDPRs krav (Datainspektionen, 2017d).

Tidigare har hanteringsreglerna i Personuppgiftslagen endast behövt tillämpas på behandling av strukturerade personuppgifter. Anledningen bakom varför dessa hanteringsregler enbart gäller för strukturerade personuppgifter och inte ostrukturerade, är på grund av att det har önskats att underlätta för vardaglig hantering som inte medför integritetsrisker. Detta medför att ostrukturerad behandling mer eller mindre får lov att utföras fritt, så länge som uppgifterna det gäller inte blir kränkta (Datainspektionen, 2017e). Med GDPR försvinner alltså både missbruksregeln och PuL med dess hanteringsregler och samtliga krav inom GDPR kommer att gälla både för strukturerad och ostrukturerad data.

2.8 Andra krav i GDPR

Rätt till radering ('Rätten att bli glömd')

GDPR ger samtliga medborgare i EU rätt till radering, eller 'Rätten att bli glömd' som det också formuleras. Detta innebär att samtliga personer har rätten att vända sig till det företag eller den myndighet som behandlar individens personuppgifter och be om att de personuppgifter som avser henne eller honom raderas. Raderingen av personuppgifter sker dock endast i särskilda fall och dessa är följande:

- I det fall att uppgifterna som samlats in inte längre behövs för det ursprungliga ändamålet de samlats in för
- Vid återkallat samtycke från den individ vars personuppgiftsbehandling grundar sig på individens samtycke
- Om syftet med behandlingen är för direktmarknadsföring och individen vars data behandlas motsätter sig behandlingen
- Personuppgiftsbehandling inom ramen för myndighetsutövning, eller efter intresseavvägning där individen motsätter sig personuppgiftsbehandlingen och det saknas skäl som väger tyngre än intresset hos individen vars personuppgifter det gäller
- För uppfyllande av en rättslig skyldighet där radering krävs för att åstadkomma detta
- I det fall att personuppgifterna gäller ett barn och insamling har gjorts genom att barnet i ett socialt nätverk har skapat sig en profil
  (Datainspektionen, 2017f)

Den registrerades rätt till tillgång (’Rätten till information’)
Detta krav möjliggör för individen att få reda på vilka personuppgifter som behandlas som rör dem. Det innebär också att individen skall få tillgång till personuppgifterna, samt få reda på avsikten med behandlingen. Kravet innebär även att individen har rätt till att få veta vilka kategorier som personuppgifterna faller under, under vilken period som behandlingen kommer ske (om applicerbart), vem mottagaren av personuppgifterna är m.m. (Europaparlamentets och rådets förordning (EU) 2016/679) (Datainspektionen, 2017i).

Om uppgifterna inte inhämtats från individen i fråga, ska information ges för vart de hämtats. Företag som bedriver profilering eller någon form av automatiserat beslutsfattande ska informera personer om detta. Inkluderat ska individen informeras om rätten till radering, begränsning av behandling, samt rätten till rättelse. De har även rätten att klaga till en tillsynsmyndighet (Europaparlamentets och rådets förordning (EU) 2016/679).

Dataportabilitet
Med GDPR tillkommer även dataportabilitet. Detta innebär att den person vars uppgifter har lagrats för att uppfylla ett avtal eller som lagrats med samtycke, har rätten att få ut sagda uppgifter för att föra över dem till en annan tjänst om så önskas. Personen i fråga har alltså rätten att begära att information som de tidigare givit, flyttas över till en annan personuppgiftsansvarig, exempelvis ett annat företag eller tjänst, där det är tekniskt möjligt (Europaparlamentets och rådets förordning (EU) 2016/679).

Konsekvensbedömning
Det andra som är nytt och som måste följas är konsekvensbedömning. Detta görs när det ska ske en ny behandling av personuppgifter som kan innebära risker för de vars uppgifter registreras. En bedömning över potentiella konsekvenser som kan uppstå genom behandlingen av de specifika personuppgifterna måste utföras. Denna bedömning följs sedan av att organisationen tar fram åtgärder för att minimera riskerna (Europaparlamentets och rådets förordning (EU) 2016/679) (Datainspektionen, 2017a).

Anmälan av personuppgiftsincident
Om en säkerhetsincident inträffar, exempelvis en förlust av uppgifter eller dataintrång, ska detta anmälas till Datainspektionen inom 72 timmar. Detta kallas för en ’anmälan av personuppgiftsincident’ och kan även innebära att de personer vars uppgifter det gäller ska informeras. Inom varje organisation som behandlar känsliga uppgifter, exempelvis myndigheter, krävs det att ett dataskyddsombud utses. Dataskyddsombudet kommer vara en person inom organisationen som har som särskild uppgift att bevaka dataskyddsfrågor (Europaparlamentets och rådets förordning (EU) 2016/679) (Datainspektionen, 2017h). Det blir därmed viktigt att organisationen och verksamheter kan påvisa till Datainspektionen, vilka rutiner de följer om en eventuell personuppgiftsincident skulle inträffa.

2.9 Checklistor

Checklistor finns i flera olika former inom flera olika branscher beroende på det syfte den ska användas till. Användning av checklistor kan ofta ses inom kritiska yrken, såsom medicin och flygbranschen. Checklistor förekommer ofta inom medicin där de används för att se till att riktlinjer följs som de ska. World Health Organization (WHO) skapade en checklista kallad ”Surgical Safety Checklist” som designades för att försöka minska komplikationer och dödsfall under operation. Detta genom att checklistan skulle bidra till förbättrad kommunikation och följdriktighet inom de olika team av läkare och kirurger som utför operationerna (Haynes, et al., 2009). Checklistor används även inom flygbranschen där piloter bockar av en checklista innan de lyfter. Detta anses vara standard att genomföra för att bibehålla säkerhet i flygplanets cockpit (Degani & Wiener, 1993). Desto svårare är det att hitta checklistor i koppling till IT-branschen och det kan tänkas att checklistor kan användas som hjälpmedel även inom IT. Checklistan kan då bidra till att hålla arbetssysslor konsekventa och se till att de genomförs. Det kan även tänkas att en checklista kan fungera som en påminnelse om vad som behövs göras.

2.10 Relaterad forskning

Relaterad och tidigare forskning inom GDPR har inte gjorts i en större utsträckning. Det är troligt att detta främst beror på att mer forskning görs efter att en lag har trätt i kraft för att se hur lagen påverkat det ena eller det andra. Eftersom GDPR träder i kraft i maj i år, kan det tänkas att allt mer forskning kommer att göras inom området efter detta datum.

2017 gjordes två arbeten inom området GDPR som denna studie förhåller sig mot, varav ett också behandlade metoden Privacy by Design. Karlström (2017) utförde sitt arbete med syftet att ta fram vilka förberedelser organisationer kan tänkas behöva ta till i sitt arbete inför dataskyddsförordningen. Gentemot detta arbete skiljer sig Karlström (2017) i det att hans arbete syftade att kunna appliceras både organisatoriskt och tekniskt. Hans arbete skiljer sig även i att resultatet bestod av ett ramverk som användes för att mäta organisationers mognadsgrad inför GDPR. Detta arbete tar istället fram en checklista och tittar enbart på den tekniska påverkan som GDPR ställer mot befintliga informationssystem. I likhet med detta arbete användes ramverket i Karlström (2017) arbete för att ta fram hur organisationer bäst kan förbereda sig inför dataskyddsförordningen. Detta arbete har dock som avsikt att formulera dessa förberedelser i form av frågor och rekommendationer i en checklista, där Karlström (2017) tog fram förberedelseaktiviteter. Han utförde sitt arbete med intervjuer, kvalitativa enkäter och test av ramverket.

Rännare (2017) skrev sitt arbete med fokus på Privacy by Design genom Ann Cavoukians filosofi. Hon undersökte om en organisation förhåller sig till och matchar denna filosofi i sin implementation. Hennes arbete hade som syfte att undersöka den påverkan GDPR ställer på en organisation som arbetar med mjukvaruutveckling samt informationssäkerhet, utifrån ett systemadministratörperspektiv. Likhet ligger i att även

detta arbete fokuserar på Privacy by Design och de sju grundläggande principerna, men går inte in djupare in i Cavoukians filosofi. Istället bemöts enbart de grundläggande principerna för att se om de går att identifiera i organisationers tekniska arbete. Rännare (2017) bemötte både organisatoriska och tekniska aspekter och hon tog upp mer om informationssäkerhet och frågor kring integritet. Detta skiljer sig från detta arbete som fokuserar på befintliga informationssystem inom organisationer. Rännare (2017) har också använt intervjuer och genomförde arbetet inom en organisation. Skillnad finns i att hon utförde mer strukturerade intervjuer i samband med en fallstudie. Intervjuerna skedde enbart inom en och samma organisation inom informationssäkerhetsbranschen. Detta arbete använder istället semistrukturerade, öppna intervjuer där intervjuerna sker på flera olika organisationer. Detta arbete kombinerar även intervjuerna med observation som en ytterligare datainsamlingsmetod, där Rännare (2017) istället använde sig av litteraturgranskning. Hennes arbete utgick även från färdigformulerade hypoteser, där detta arbete istället strävar efter att som resultat kunna formulera en teori.

Likhet finns för det förväntade resultatet där Rännare (2017) tog fram hur en organisation förbereder sig och vad som krävs för att uppfylla krav relaterade till Privacy by Design inom GDPR. Hon tog fram rekommendationer åt en organisations förberedelsearbete för hur detta kan utvecklas och förbättras. Detta arbete syftar istället att ta fram rekommendationer i relation till Privacy by Design och hur principerna enklare kan uppfyllas, kombinerat med mognadssteg för krav inom förordningen. Vidare gjorde Rännare (2017) ingen avgränsning för vilken typ av system som arbetet berörde eller om det förväntade resultatet skulle vara applicerbart för både nyutveckling och befintliga, färdigutvecklade system. Detta arbete avgränsar sig till att endast studera befintliga informationssystem.

3 Problemområde

Detta kapitel beskriver den frågeställning och problematik som ska besvaras. Problemområde, frågeställning och avgränsningar tas upp, samt förväntat resultat.

Den tekniska utvecklingens framfart har lett till en ökad användning och registrering av personuppgifter. Dessa personuppgifter används på flera olika enheter och i många olika system. Med detta upplevs även en ny trend ha tagit form, där ett stort fokus ser ut att finnas för hur personuppgifter kan säljas vidare eller användas vid riktade erbjudanden och reklam, för att bidra till ökade intäkter. Personuppgifter idag kan nästan ses som något som har ett kommersiellt värde.

När personuppgifter för jämnan sparas, registreras och behandlas i vart och vartannat system ger det upphov till ifrågasättande av hur säkra dessa personuppgifter egentligen är. I Sverige har Personuppgiftslagen (PuL) fungerat som ett skydd av individens personuppgifter. Detta förändras från och med 25 maj 2018 då det istället är GDPR som står för skyddet av personuppgifter och individens integritet, eftersom GDPR ersätter PuL. Den nya dataskyddsförordningen kommer leda till ett utökat skydd av individers personuppgifter, men det kommer sannolikt innebära stora förändringar för många företag och myndigheter runt om i världen. Då många olika företag och verksamheter hanterar åtminstone någon personuppgift såsom till exempel personnummer, telefonnummer, e-postadress eller IP-adress, kommer en stor mängd organisationer bli påverkade.

GDPR kommer ställa nya och högre krav på hur personuppgifter behandlas både i företag och i de system som används. Det blir därmed av intresse att ta reda på hur stor effekt GDPR kommer ha på befintliga system - hur illa kan det tänkas att systemen som används idag ligger till? Det vill säga, om det finns stora svårigheter för hur vissa krav ska bemötas tekniskt i och med att några krav inom förordningen potentiellt kan vara krångligare än andra att anpassa befintliga informationssystem efter. Alternativt, om något krav till och med upplevs som omöjligt att utföra. Det blir även intressant att se om där finns krav som påverkar dessa informationssystem mer och gör att organisationer inte ligger i fas med förordningen. Detta medför att det finns en betydelse i att undersöka hur organisationer idag förbereder sig och anpassar sig till den nya lagtexten. Detta arbete har som syfte att undersöka den nya dataskyddsförordningen GDPR och de krav som denna lag kommer ställa på befintliga informationssystem. Studien kan då ta reda på om där finns utmärkande punkter som är mer eller mindre besvärliga att hantera rent tekniskt.

I och med att krav inom GDPR utgår från metoden Privacy by Design kommer studien ha ett fokus på denna metod. Studien har för avsikt att ta reda på hur väl de sju grundläggande principerna inom Privacy by Design tillämpas inom organisationer. Det blir intresseväckande att undersöka om där är principer som oftare anses att de uppfylls. Studien kommer därmed även undersöka hur Privacy by Design i relation till GDPR lämpligen kan tillämpas på befintliga informationssystem. Detta kan även tänkas

leda till att studien kan identifiera ett genomgående mönster för vilket eller vilka krav eller principer som informationssystem brister på.

För att ge en bild över hur väl olika företag förbereder sig inför GDPR har flertal enkäter gjorts. En enkät gjord av TrustArc i 2017 frågade 200 företag inom flera olika områden, om deras förberedelse inför GDPR. I denna enkät svarade 61% med att de ännu inte hade påbörjat sin förberedelse inför den nya förordningen (TrustArc, 2017). I november 2017 utfördes en ny studie där en ny enkät gavs ut åt företag att besvara. Denna enkät gjordes av föreningen ”iapp” i samarbete med TRUSTe, numera TrustArc, där 67% svarade att de hade påbörjat implementering inför GDPR (Chiavetta, 2017). Detta tyder på att det är troligt att flertal företag har bristande informationssystem som behöver ses över och att många företag ligger efter i sin förberedelse. Studien baseras därmed på antaganden om att många befintliga informationssystem som hanterar personuppgifter ännu inte är redo och har uppdaterats inför GDPR.

Ett samarbete med ett IT-konsultbolag som under studiens gång arbetar med att vara i linje med GDPR, kan tänkas ge forskaren en bild av hur ett förberedande arbete inför GDPR kan se ut. Studien kommer undersöka ett befintligt informationssystem hos IT-konsultbolaget som driftar systemet, för att se hur det uppdateras och förändras. Det kan även bli en fråga om hur både interna och externa informationssystem säkras för att uppfylla kraven GDPR ställer. Det befintliga informationssystemet är ett system som brukas inom fordonsbranschen och hanterar stora mängder personuppgifter i form av kunddata. Systemet innefattar bland annat funktionalitet för att hantera kunder, bokning av testkörning, offerthantering och skapande av kontrakt. Kraven för individers integritet måste vara sammanhängande med informationssäkerheten i en organisation, samt hur personuppgifter behandlas. Hur detta kan behöva förändras är en intresseväckande fråga som behöver ses över. Genom observation och intervjuer kommer data samlas in för att ta reda på om där finns krav som upplevs som svårare att bemöta för organisationers befintliga informationssystem. Detta kommer även kombineras med att studera hur Privacy by Design kan knytas an bättre till GDPR-förberedelse och användas för att informationssystem bättre ska gå i linje med det som GDPR kräver.

3.1 Problem/fråga

Baserat på det tidigare diskuterade problemområdet har följande frågeställning tagits fram för att bli besvarad i detta arbete:

"Hur påverkas befintliga IT-system av GDPR och Privacy by Design och hur kan en checklista användas för att avgöra hur redo ett system är för GDPR?"

Denna fråga innebär därmed att undersöka hur befintliga system ligger till inför att GDPR träder i kraft och se om det finns krav som påverkar mer eller mindre. Inkluderat undersöks det även huruvida det går att tillämpa de sju grundläggande principerna inom Privacy by Design. Detta kommer sedan utvecklas till en checklista som kan ge en bild av hur redo ett system är.

Huvudfrågan delas upp i två delfrågor som bemöts under forskningsprocessen för att hjälpa besvara huvudfrågan. Dessa delfrågor formuleras på följande vis:

1. *"Vilka är de viktigaste kraven inom GDPR för befintliga informationssystem?"*

2. *"Hur väl går de sju grundläggande principerna inom Privacy by Design att uppfylla för befintliga informationssystem?"*

3.2 Avgränsningar

Eftersom GDPR är en omfattande förordning som berör organisationer, verksamheter och myndigheter på många olika sätt, görs en avgränsning för hur stor del av GDPR som kommer undersökas. Det primära fokuset kommer ligga på de krav inom GDPR som har relation eller relevans till Privacy by Design. I och med att Privacy by Design är en etablerad metod som kan kännas igen på många håll inom systemutveckling, samt att det är en metod baserad på personlig integritet, blir det därmed ett intressant område för författaren att fördjupa sig i.

Studien kommer inte gå in på djupet för vilken påverkan GDPR generellt har på en organisation. Exempelvis kommer tillkommande kostnader från förberedelse inför GDPR inte vara något som studien berör. Påverkan på arbetsprocesser, nätverksarkitektur eller fysiska utrymmen som kan komma av GDPR är heller inte något som studien kommer att bemöta. Arbetet kommer enbart att besvara vilken påverkan GDPR kan tänkas ge på befintliga informationssystem som redan är i bruk. Studien kommer inte att undersöka hur nyutveckling av nya system berörs.

En avgränsning görs även för vilken typ av system det är som aktivt kommer att observeras. Studien kommer inte att studera alla olika system som finns, då detta är ett för stort antal system som är allt för omfattande att bemöta. Fokus ligger istället på enbart ett system för att sedan kombinera information från observation av systemet med intervjuer. Det system som kommer användas i datainsamlingen är ett befintligt informationssystem som används inom fordonsbranschen och driftas, samt förbereds inför GDPR av den organisation som författaren utför studien hos. Detta informationssystem hanterar stora mängder kunddata och fordonsinformation, samt

har olika funktioner för olika användare av systemet. Systemet innefattar även en front end-del i form av en hemsida som samlar in kunddata. Det ingår även funktionalitet för offerthantering, skapande av kontrakt, bokning av testkörning m.m.

Gällande cyberbrott med direkt koppling till personuppgifter såsom läckage av känslig information på grund av hackare, eller identitet och integritetsbrott är ytterligare ett område där studien gör en tydlig avgränsning. Studien kommer inte gå närmare in på cyberbrott. Detta eftersom ett beslut togs för att cyberbrott har större relevans till informationssäkerhet än till GDPR. I och med att detta arbete koncentrerar sig på GDPR som ämne är inte relevansen hög nog att gå djupare in på integritetsbrott eller andra cyberbrott.

3.3 Förväntat resultat

Efter att det insamlade materialet från observationer och intervjuer har analyserats, förväntas resultatet bli en checklista. Denna checklista är tänkt att vara applicerbar på befintliga informationssystem och blir något som systemägare kan agera på, något som är handlingsbart. Själva förordningen är stor och mycket att sätta sig in i. Detta kan göra att det blir svårt för systemägare att veta vad som är viktigast för dem och vad de bör lägga fokus på. Checklistan kan därmed fungera som en sammanfattning eller summering av vad GDPR säger och innebär, samt hur Privacy by Design kan inkluderas i informationssystemet.

Genom arbetets inriktning mot Privacy by Design förväntas studien kunna identifiera mönster för hur de sju grundläggande principerna inom metoden används av organisationer eller inte. Det är även troligt att detta kan ha en påverkan på det förberedande arbetet inför GDPR. Författaren gör även ett antagande att fler utmärkande utmaningar för att uppfylla vissa krav inom GDPR kan tänkas finnas hos olika organisationer.

Checklistan kommer baseras den analys som görs av insamlade data, för att fastställa vilka olika svårigheter GDPR kan medföra. De krav som identifieras som de mest väsentliga att bemöta i befintliga informationssystem kommer i checklistan presenteras med var sin fråga. Till frågorna kommer det ges svarsalternativ i form av tre steg. Varje svarsalternativ kommer representera en nivå av mognadsgrad. Dessa tre steg kan tänkas fungera som en anvisning om hur organisationer bättre kan vara i linje med förordningen. De sju grundläggande principerna inom Privacy by Design kommer att ingå i en separat del av checklistan. Varje princip ges tillhörande rekommendationer om hur den bäst uppfylls. Dessa rekommendationer kommer baseras på insamlad data och litteratur. Checklistan kommer ge systemägare riktlinjer för vart de bör koncentrera sitt GDPR-arbete för befintliga informationssystem. Rekommendationerna kan sedan hjälpa systemägare och organisationer för hur de ska gå tillväga för att bättre uppfylla Privacy by Design. Detta kan även bidra till att organisationen är i bättre linje med förordningen.

4 Metod

Detta kapitel beskriver valet av den vetenskapliga metod som har använts, vilka moment som ingår och dess utförande. Kapitlet tar även upp validitet och reliabilitet av metod och data som samlats in, samt etiskt ställningstagande.

4.1 Metodval

Efter att en problemformulering var gjord och en frågeställning var formulerad blev nästa steg att välja en lämplig, vetenskaplig metod för arbetet. Som Berndtsson, Hansson, Olsson och Lundell (2008) beskriver det, är metodvalet betydelsefullt för att slutförandet av rapporten ska vara lyckat. Metoden innehåller proceduren, medlet och tekniken för hur en process ska utföras på ett systematiskt, logiskt och metodiskt sätt (Berndtsson, et al., 2008). De beskriver en metod inom ett forskningsprojekt på följande vis:

"… ett organiserat tillvägagångssätt för problemlösning som inkluderar (1) insamling av data, (2) formulering av en hypotes eller en tes, (3) testande av hypotesen, (4) tolkning av resultatet, och (5) fastställa en slutsats som senare kan utvärderas självständigt av andra." (Berndtsson, et al., 2008, p. 12)

Kvalitativ forskning

Valet föll på att använda en kvalitativ metod med induktiv ansats där intervjuer och observation blir studiens datainsamlingsmetoder. Detta val grundades i författarens önskemål om att komma närmre fenomenet i form av kontakt med personer som i dagsläget arbetar med förberedelse inför GDPR. Genom att använda olika datainsamlingsmetoder och på så sätt få in olika data, skapas triangulering som kan bidra till att bättre belysa hur de olika metoderna och olika typer av data stödjer varandra.

Creswell och Clark (2007) lyfter att syftet inom kvalitativ forskning är att förstå den betydelse som individer ger till ett visst fenomen. Användandet av litteratur har inte lika stor roll, utan används för att rättfärdiga det problem som undersöks. Författarna beskriver hur syftets fokus sker genom att forskaren ställer öppna frågor för att försöka förstå den komplexitet som finns bakom en idé eller ett fenomen. Datainsamlingen sker därmed genom ord eller bilder och från ett färre antal deltagare och forskningsplatser. Denna datainsamling beskriver även författarna kan ske genom observation av exempelvis en deltagare som undersöks vid den plats de av naturliga skäl vanligtvis befinner sig. Den data som samlas in analyseras sedan genom bildanalys eller textanalys. Forskaren tittar då efter större mönster, teman eller generaliseringar. Författarna tar även upp att forskarens roll inom kvalitativ forskning går ut på att identifiera en personlig ställning i problemet eller frågan och kunna rapportera om där finns partiskhet. För att sedan validera data görs detta genom olika valideringsprocedurer som förlitar sig på deltagare, forskaren eller läsaren (Creswell & Clark, 2007).

4.2 Intervjuer

Bell (2000) beskriver att en stor fördel med intervjuer är den flexibilitet de har. Hon menar att en skickligt utförd intervju kan undersöka svar, gå djupare in på känslor och motiv, samt följa upp idéer som beskrivs (Bell, 2000). Intervjuer kan fungera som kraftfulla verktyg som hjälper till att förstå behov och utmaningar, till trots att de har sina begränsningar. För att genomföra effektiva intervjuer krävs det att intervjupersoner noggrant väljs ut, samt hur intervjuprocessen ska struktureras. Intervjuer kan vara helt strukturerade, ostrukturerade eller semistrukturerade, beroende på vad som passar situationen och/eller forskning bäst (Lazar, et al., 2017).

Berndtsson et al. (2008) lyfter vikten av en noga utvald intervjumetod och menar att det finns flera aspekter som behöver tas i åtanke när en intervjumetod ska väljas. Författarna fortsätter med att beskriva hur olika typer av intervjuer har olika styrkor och svagheter och hur dessa behöver en god koppling till forskarens förmåga att utföra intervjuer. Inom kvalitativ forskning förekommer ofta öppna intervjuer. För denna intervjumetod förklarar författarna vidare att det finns liten eller ingen kontroll hos forskaren för vilka problem som kommer tas upp i intervjun (Berndtsson, et al., 2008).

I öppna intervjuer ställs frågorna på ett sådant sätt att de, som Berndtsson et al. (2008) förklarar, ”öppnar upp” för viktiga spörsmål eller problem. I och med detta undviks slutna frågor som enbart genererar ”ja/nej”-svar. För att undvika svagheten att inte kunna behålla möjligheten för att ändra eller ta bort frågor beroende på de svar som ges, undviks en stängd intervju. I slutna eller ”stängda” intervjuer används fastställda frågor, vilket är ett passande val vid enkätundersökningar där ett statistiskt resultat önskas tas fram (Berndtsson, et al., 2008).

Studien kommer att använda öppna intervjuer med en semistrukturerad intervjumetod och ett avsiktligt urval av respondenter. En semistrukturerad intervju är ett lämpligt val eftersom forskaren önskar ställa frågor kring särskilda teman i samtliga intervjuer. Till största del kommer intervjun bestå av öppna frågor med stort utrymme för följdfrågor. Detta medför att vissa frågor kan komma att ändras, tas bort eller läggas till utefter svaren som intervjupersonerna ger. Detta passar studiens syfte bra, då frågor relaterade till studiens syfte kan behållas i samtliga intervjuer och på så sätt hålla intervjun inom forskningens ämne. Samtidigt ger detta intervjupersonerna möjligheten att ge friare svar som i sin tur kan ge upphov till olika typer av följdfrågor.

Vid förberedelsen inför en intervju beskriver Bell (2006) hur forskaren bör välja ut väsentliga teman och frågeställningar som önskas att besvaras. Detta följs sedan av att forskaren utformar frågor och utför en eller ett par pilotintervjuer. Hon tar även upp vikten av att etablera en god kontakt med intervjupersonen (Bell, 2006). Genom att utföra kvalitativa intervjuer kan informationsvärdet öka och leda till att en grund för uppfattningar och tankar om det fenomen som studeras skapas. Denna grund hos forskaren kan då bli mer fullständig och gå djupare än den annars gjort (Holme & Solvang, 1997).

Val av relevanta intervjupersoner

Då urvalet för intervjupersonerna kommer göras avsiktligt baseras detta på personer som kan besvara intervjufrågorna utifrån både en teknisk synvinkel, samt med viss kunskap om GDPR. Därmed kommer urvalet bestå av personer som har någon form av teknisk bakgrund eller som aktivt är involverade i organisationens arbete med GDPR. Vid val av intervjupersoner ligger fokus på de som inom organisationen arbetar med systemutveckling av något slag. Detta kan vara i form av systemutvecklare, IT-konsult eller systemarkitekt. Intresse ligger även i att eventuellt utöka urvalet och intervjua IT-ansvariga, samt säkerhetsansvariga, exempelvis CIO och VD. Utöver detta kommer även en annan person intervjuas - en praktikant som på samma organisation där studien utförs, också genomförde ett arbete med inriktning mot GDPR.

Planering av interaktion och struktur under intervjun

I och med att valet hade gjorts att använda en semistrukturerad intervjumetod, kommer en intervjuguide att struktureras upp. Detta kommer göras på ett sådant sätt att den underlättar för både interaktion och struktur av intervjun. Exempelvis kommer intervjun börja med inledande frågor för att skapa god kontakt och tillförlitlighet med intervjupersonen. Därefter kommer frågorna gå vidare till mer generella frågor kring organisationens GDPR-arbete, för att sedan gå in mer på djupet i hur organisationen arbetar rent tekniskt. Frågorna kommer även beröra vilka utmaningar som kan tänkas ha uppstått i GDPR-arbetet. Avslutningsvis kommer frågor om Privacy by Design att ställas. Bland annat kommer intervjupersonerna bli tillfrågade om de vet med sig att organisationen arbetar enligt någon av de sju grundläggande principerna.

Insamling och strukturering av svar under intervjun

Insamlingen av svaren under intervjun kommer göras med papper och penna. De anteckningar som tas kommer vara i form av förkortade versioner av det som sagts. Svaren kommer kortas ner för att kunna ge intervjupersonen och intervjun tillräckligt med uppmärksamhet och för att inte skapa en distraktion i att skriva ut samtliga svar ordagrant. För att fånga upp sådant som potentiellt kan ha missats, kommer samtliga intervjuer spelas in om tillåtelse för detta ges av intervjupersonen.

Inspelning av intervjun

I och med att intervjuerna är semistrukturerade och innehåller öppna frågor, medför detta att helt korrekta och ordagranna anteckningar kan vara svårt att hinna med. För att säkerställa att all information från intervjuerna fångas upp kommer intervjupersonen tillfrågas om de ger tillåtelse för att intervjun spelas in. Varje intervjuperson blir tillfrågad om de accepterar att inspelning sker, med fullständig möjlighet att tacka nej om så önskas. Inspelningarna ger sedan underlag för transkribering av intervjuerna.

Konfidentialiet
Då studien genomgående tar hänsyn till individskyddskravet, medför detta att konfidentialitet ska bevaras. Samtlig information som samlas in ska förvaras på ett sådant sätt att ingen obehörig kan få tillgång till den. Insamlad information kommer sparas och presenteras på ett sådant sätt att ingen identifiering ska vara möjlig. De ljudinspelningar som kommer göras vid utförande av intervjuer kommer ske med hjälp av forskarens privata mobiltelefon och hålls säkra på mobiltelefonen genom att ett längre lösen eller fingeravtryck krävs för upplåsning. Ljudinspelningarna kommer efter varje intervjutillfälle att föras över från mobiltelefon till forskarens privata dator där det också enbart är forskarens själv som har tillgång till lösenordet.

Ingen annan direkt personuppgift kommer samlas in under intervjuerna då denna typ av information inte behövs för att uppfylla studiens syfte. Däremot kan indirekta personuppgifter som kan härledas i samband med ytterligare information fångas upp i anteckningar under intervjun utifrån de svar som ges. Hänsyn kommer tas till denna risk genom att anteckningar görs med material som enbart kommer användas vid intervjuerna. Därefter kommer anteckningarna att hållas inom forskarens egna privata ägor där utomstående inte har tillgång till dem. Hänsyn kommer även tas för att hålla transkriberat material säkert. Direkta personuppgifter kommer inte att tas med i transkriberingen, utan varje intervjuperson anonymiseras genom att bli kallad ”Respondent X” där X står för en siffra. Det transkriberade materialet kommer sedan att sparas enbart på forskarens privata Google Drive där det endast är forskaren själv som har tillgång till lösenord och verifiering för att komma åt materialet. På detta vis kan en extern anonymitet av intervjupersonerna upprätthållas genom studien. Detta eftersom det ej blir möjligt att identifiera intervjupersonerna utanför deras organisation. Extern anonymitet kommer därmed att hållas kontinuerligt under hela studien. Vidare bör det uppmärksammas att intern anonymitet för vem som deltar i intervjuerna på de externa företagen kommer upprätthållas om det efterfrågas. Intern anonymitet är inte efterfrågat inom den organisation forskaren utför studien på och forskaren kommer därför inte upprätthålla detta för organisationens respondenter.

Val av plats för intervjun
Av de intervjuer som kommer göras, är forskarens ambition att utföra åtminstone hälften av intervjuerna på den organisation som är studiens datakälla. Detta blir ett lämpligt val då intervjupersonerna kommer kunna känna sig bekvämare i och med att de kommer befinna sig i en bekant miljö. Åtminstone två av de externa intervjuerna kommer ske på det företag som är arbetsplats för intervjupersonerna i fråga. Detta eftersom intervjupersonerna på så vis kan känna sig mer komfortabla i en välbekant omgivning. Utöver en behagligare situation åt intervjupersonen, baseras detta val även på att underlätta och undvika allt för stor tidsåtgång i form av resväg för intervjupersonen.

Transkribering
Eftersom intervjuerna kan komma att spelas in, blir följden transkribering av samtliga inspelningar. Vid transkribering görs valet att ej ta med skratt, pauser, harklingar m.m. i transkriberingen, eftersom detta inte är information som är av någon vikt för studiens syfte. Det som transkriberas kommer vara de frågor och följdfrågor som ställs, samt de svar som gavs, men i förenklad form. Detta innebär att felsägningar och upprepande av samma ord inte heller tas med i transkriberingen.

När en intervju är transkriberad och klar skickas materialet ut till respektive respondent för att ge möjlighet att se om det som sagts blivit uppfattat korrekt. Vidare ges respondenterna även möjligheten att tillägga något om de önskar, men samtliga av dessa saker kommer vara frivilliga.

4.2.1 Frågekonstruktion

Jacobsen (1993) beskriver hur viktigt det är att skilja på öppna och slutna, eller vida och snäva, frågor i en intervju. För att avgöra om en fråga är öppen eller sluten gäller det att titta på karaktären på själva utrymmet som svaret har. Detta innebär att om det finns flera svarsmöjligheter är utrymmet större och frågan är därmed mer öppen. Fortsättningsvis beskrivs det hur öppna frågor uppmanar den som svarar att ge utryck för en åsikt. Detta gör att det blir lättare för forskaren eller intervjuaren att hitta något att gå vidare med i de svar som ges, om frågorna som ställs är mer öppna. Författaren menar att när det finns mer att välja mellan kan en intervju bli mer *"sammanhängande och inrymma en dimension av utveckling och dynamik."* (Jacobsen, 1993, p. 101).

Intervjufrågor
Ahrne och Svensson (2011) lyfter att det i intervjuer är betydelsefullt att intervjuaren är tydlig med att visa intresse och vill ta del av det intervjupersonen berättar, samt att ställa vänliga frågor. Författarna fortsätter med att säga att om det upplevs att ett svar kräver mer förklaring kan frågan upprepas, men gärna omformulerad. Detta ger intervjupersonen betänketid och de kan sedan berätta igen. Vid följdfrågor lyfter författarna även tekniken att använda intervjupersonens egna ord för att på så sätt möjliggöra för intervjupersonen att berätta mer då de känner sig tryggare (Ahrne & Svensson, 2011). Samtliga tekniker kommer hållas i åtanke under både utformande av intervjuguide, men även under intervjutillfällena. Detta kan tänkas leda till att intervjusituationen blir mer bekväm för bägge parter, samt kan leda till mer informationsrika svar.

Intervjun kommer struktureras upp med inledande frågor, några generella frågor kring GDPR-arbetet som utförs, för att sedan gå mer in på djupet i tekniska frågor. De inledande frågorna ställs för att etablera bättre kontakt med intervjupersonen. Detta kan tänkas underlätta för intervjupersonen och göra det enklare för intervjupersonen delta i intervjun, genom att de får prata om något vardagligt och om sig själva. På detta sätt kan intervjun tänkas bli mindre sträng eller intensiv, där intervjupersonen inte känner att de är i en lika utsatt position. De tekniska frågorna kommer formuleras efter

de krav i GDPR som studien koncentrerar sig på. Vidare följs de tekniska frågorna av spörsmål relaterade till metoden Privacy by Design och dess sju grundläggande principer.

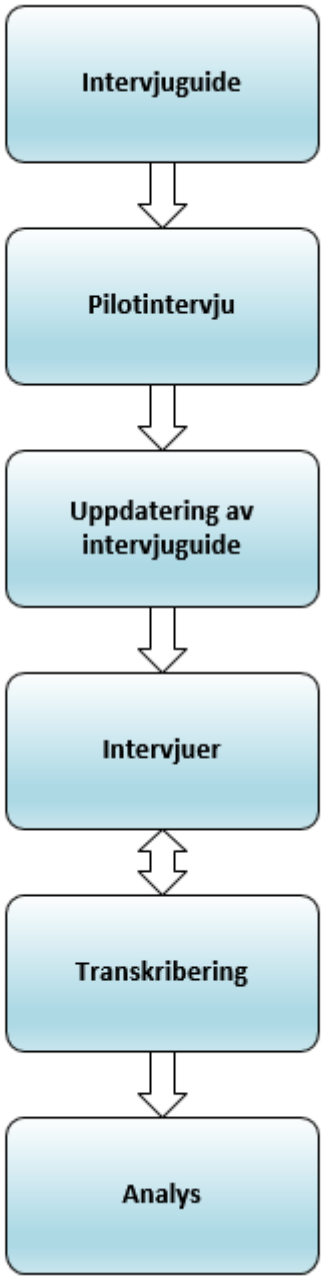
Intervjuguide

Efter att studiens upplägg, samt intervjuformen var bestämd, blev nästa steg att utforma vilka frågor det var som skulle ställas i själva intervjun. Lantz (1993) skriver hur just detta steg gärna är enklare än att problematisera. Detta i och med att värdet är avhängande på hur frågorna har arbetats fram för att nå den slutliga formuleringen (Lantz, 1993). I detta steg utformas en intervjuguide med till största del öppna frågor som hålls inom det utarbetade problemområdet. De frågor som kommer ställas formuleras på ett sådant sätt att intervjupersonen själv kan ge ett mer utökat svar om hur de tycker och tänker. Intervjuguiden har även rum för potentiella följdfrågor.

Öppna intervjuer kan beskrivas som intervjuer med vida frågor där forskaren under intervjuns gång går in allt mer på djupet i frågorna. Som Lantz (1993) skriver, *"utan en intervjuplan är det lätt att glida iväg och skifta fokus"* (Lantz, 1993, p. 64); där hon menar att när intervjun kommit igång kan både intervjuare och intervjupersonen komma in på andra samtalsämnen som inte nödvändigtvis tillhör det ursprungliga ämnet i intervjun. För lite mer riktning kan en riktad öppen intervju användas, vilket har utrymme för följdfrågor inom frågeområdet som ställd mot den bakomliggande förståelse som forskaren/intervjuaren har (Lantz, 1993). I intervjuguiden kommer ett par enskilda frågor som är mer strukturerade och inte lika öppna, fortfarande ställas. Även dessa frågor ger utrymme för följdfrågor för att samla in ytterligare tankar och tyckande från intervjupersonerna. Frågorna ställs på ett sådant sätt att intervjupersonen kommer ombeds berätta vad de har för syn på något, eller vad de har för tankar om olika delar med relevans till forskningsområdet.

Pilotintervju

Efter att intervjuguiden har arbetats fram kommer den testas genom en pilotintervju. Reis och Judd (2000) tar upp att mer strukturerade pilotintervjuer är användbara vid utformande av punkter och frågor till ett frågeformulär (Reis & Judd, 2000). Pilotintervjun kommer utföras för att testa intervjuguiden och se hur väl frågorna fungerar i praktiken. Detta kan då uppmärksamma om någon fråga behöver formuleras om. Eventuell omformulering kommer bero på oklarhet där intervjupersonen inte förstår frågan, om någon fråga ger upphov till ja och nej-svar, samt om de svar som ges är det studien efterfrågar eller inte. Efter pilotintervjun får respondenten som agerar pilot även ge kritik och tankar om hur intervjun har utförts. Det som framkommer från pilotintervjun kommer ligga i grund till eventuell omarbetning av intervjuguiden. Utöver omformulering av frågor kan omarbetning även vara i form av uppdaterad struktur av följden på frågorna.



Figur 2 – **Intervjuprocess** (Författarens egna)

4.2.2 Etik

Studien tar ett etiskt ställningstagande och hänsyn kommer tas till individskyddskravet. Individskyddskravet hjälper till att skydda de personer som deltar i forskningen. Deltagande skyddas bland annat genom att de ska informeras om syftet för forskningen, att personuppgifter som samlas in inte kommer att användas i något annat syfte, att medverkan är frivillig m.m. Individskyddskravet är uppdelat i fyra kategorier, nämligen Informationskravet, Samtyckeskravet, Konfidentialitetskravet och Nyttjandekravet (Vetenskapsrådet, 2002). Bell (2006) beskriver bland annat vikten av att känna till de etiska riktlinjerna som finns vid forskning och särskilt vid utförande av intervjuer. Hon

förklarar att detta kräver medgivande från intervjupersonerna innan själva intervjuarbetet har startat (Bell, 2006).

Innebörden av att forskningen innefattar etiska aspekter, är att det skapas ett samtycke från intervjupersoner och de personer som ingår i observation. Ytterligare innebär det även att en överenskommelse finns för hur det insamlade materialet ska användas och hur resultaten kommer visas (Bell, 2006).

Informationskravet
Inför intervjun ska forskaren informera intervjupersonen om forskningens syfte. Kravet inkluderar att informera deltagande intervjuperson om villkoren för deras deltagande, samt att deras medverkan är frivillig med rätten att avbryta (Vetenskapsrådet, 2002).

Samtyckeskravet
Samtyckeskravet innebär att de som är deltagare i forskningen har rätten att själva bestämma över om de vill medverka eller inte. Forskaren behöver därför inhämta samtycke från de personer som deltar i forskningen om det är en aktiv insats från de deltagande. (Vetenskapsrådet, 2002).

Konfidentialitetskravet
Innebörden av konfidentialitetskravet är att alla uppgifter om de som ingår i studien ska ges största möjliga konfidentialitet. Deltagarnas personuppgifter ska förvaras på ett säkert sätt att inga obehöriga kan ta del av dem. Om ett forskningsprojekt omfattar etiskt känsliga uppgifter om personer som är identifierbara, bör en tystnadsplikt undertecknas. De uppgifter som samlas in om identifierbara personer ska antecknas och lagras, samt avrapporteras, på ett sådant sätt att utomstående inte kan identifiera någon person. Det ska alltså vara praktiskt omöjligt för någon som är utomstående att få tillgång till uppgifterna (Vetenskapsrådet, 2002).

Nyttjandekravet
De uppgifter som samlats in om enskilda individer i ett forskningsprojekt får endast lov att användas för forskningsändamålet. Personuppgifter får endast användas av forskaren själv. Uppgifterna kan utlånas till andra forskare, såvida de är förpliktade mot den forskare som lämnat uppgifterna, samt mot de personer som det ursprungliga materialet är hämtat ifrån (Vetenskapsrådet, 2002).

4.2.3 Urval

Valet av personer som ska intervjuas görs genom ett tvåstegsurval. I detta fall innebär det att det första är ett urval av organisationer och andra steget är urval av individer. Ahrne och Svensson (2011) lyfter hur valet av individer att intervjua ofta är beroende av ett samarbete med en ansvarig person. Den ansvariga individen har då tillgång till information och förteckningar av de anställda inom organisationen (Ahrne & Svensson, 2011). I avseende till detta samarbetar forskaren tillsammans med en ansvarig person på den organisation studien utförs på. Detta samarbete kan leda till att ta fram både organisationer och därefter individer att intervjua. En tydlig bild kan därmed ges över

vilka personer som har särskilda arbetsuppgifter eller roller inom organisationen. Ett val kan sedan baseras på detta för vilka personer som är mer relevanta att intervjua.

Ahrne och Svensson (2011) betonar även vikten av antalet intervjupersoner och menar att endast en eller ett par intervjuer sällan är tillräckligt. Författarna rekommenderar sex till åtta intervjupersoner för att öka säkerheten att det insamlade materialet är oberoende av uppfattningar som kan vara personliga för enskilda individer (Ahrne & Svensson, 2011). Ambitionen för intervjuantalet kommer ligga på sju till åtta personer plus en pilotintervju. Inklusive pilotintervjun kommer åtminstone hälften av intervjuerna utföras på det IT-konsultbolag forskaren samarbetar med.

De personer som intervjuerna kommer utföras på kommer vara personer av liknande kunskap och erfarenhet inom IT-branschen. Då målgruppen är systemägare och studien har ett tekniskt fokus är det personer med kunskap inom IT, såsom utveckling, systemarkitektur och säkerhet, som kommer väljas ut för intervju. Utöver kunskap inom IT, görs även urvalet utefter de som även besitter viss kunskap om GDPR. Strategin för urvalet är att intervjua personer som kan ge meningsfull input. Denna meningsfulla input kan ges genom att intervjua personer inom flera olika roller inom IT, men som alla kan något om GDPR. Detta kan skapa en matchning mellan de personer som ska intervjuas. Därmed skapas en bredd på de som kommer intervjuas, då de är av olika roller. De som intervjuas kommer vara allt från CIO till systemarkitekter och utvecklare. Urvalet påverkas även av möjligheten till att intervjua önskade personer, där personen i fråga behöver ha tid för att kunna ställa upp.

Ytterligare intervjuer kommer göras med personer i andra, externa organisationer. Detta skapar triangulering, då data samlas in från olika datakällor. Eftersom frågorna som formuleras i intervjuguiden kommer bemöta tekniska aspekter, blir det av stor vikt att respondenterna som väjs ut kan bidra med informationsrika svar. Detta för att ge en klarare bild över det område som undersöks. Urvalet för de personer som kommer ingå i studiens observationer, baseras på att det finns två personer som arbetar närmst och mest med det informationssystem som studien syftar att undersöka. Rollerna för dessa personer är applikationsägare, leveransansvarig och support, samt en utvecklare och programmerare.

4.2.4 Validitet och reliabilitet

Starrin och Svensson (1996) beskriver att ett mycket centralt begrepp inom både kvantitativ och kvalitativ forskning är validitet. Hand i hand med validitet talas det även om reliabilitet. Dessa begrepp kopplas till kvalitén som finns dels i datainsamlingen, men även i analysen av data. Validitet kan dock ses som överordnat reliabilitet, där Starrin och Svensson (1996) beskriver att *"...om validiteten är god är också reliabiliteten det. Men är reliabiliteten god är det inte en garanti för att validiteten också är det."* (Svensson & Starrin, 1996, p. 209).

Inom kvantitativ ansats innebär reliabilitet att vid en upprepad mätning av ett konstant objekt ges ett och samma resultat. Samma resultat kan även erhållas om en mätning görs

genom att identiska frågor ställs vid minst två tillfällen. Däremot, om frågorna inte mäter det som var syftet att mäta, blir resultaten oanvändbara till trots att det finns hög reliabilitet (Svensson & Starrin, 1996).

Reliabilitet inom kvalitativ ansats ger istället upphov till att forskaren ifrågasätter om där finns ett "konstant objekt" överhuvudtaget. Ett exempel på något som kan påverka detta är sinnestillståndet hos en respondent, något som kan variera och därmed påverka de svar som ges. Detta medför att reliabilitet bäst bedöms utifrån själva situationen vid ett intervjutillfälle. Detta till skillnad från den kvantitativa metoden där svar från samma intervjuperson från två olika tillfällen kan jämföras, är detta något som inte fungerar lika bra vid en kvalitativ ansats. Berndtsson et al. (2008) bekräftar detta och beskriver reliabilitet som riktigheten eller noggrannheten med forskarens valda metod (Berndtsson et al., 2008).

Validitet beskriver Berndtsson et al. (2008) som sambandet mellan det som avses undersökas och det som forskaren faktiskt undersöker (Berndtsson et al., 2008). Inom den kvalitativa metoden krävs det att validiteten hos frågorna bedöms i bägge situationer som de har ställts till en intervjuperson. De två begreppen, validitet och reliabilitet, blir mer sammanflätade inom en kvalitativ studie, än de blir i kvantitativa studier. Inom de kvantitativa studierna är det vanligare att titta mer på validitet, där detta begrepp anger hur väl forskaren mäter det som de har för syfte att mäta. Validitet avser hur giltiga resultaten är och hur giltigt upplägget av undersökningen, samt hur giltiga de instrument som använts är (Svensson & Starrin, 1996).

Forskaren kommer genomgående i studien ta hänsyn till bägge begrepp. Detta görs i både val av datainsamlingsmetod och hur datainsamlingen genomförs, men även under intervju och observation. Exempelvis sker detta genom det tidigare nämnda antalet intervjuer, som bidrar till att enklare kunna utesluta om svar som ges är påverkade av personligt tyckande. Genom att hålla validitet och reliabilitet i åtanke under arbetets gång, menar Berndtsson et al. (2008) att forskaren på så sätt lägger en bra grund till arbetets senare delar, såsom materialpresentation och analys. Författarna fortsätter med att säga hur detta leder till en ökad kvalitet i forskningsarbetet (Berndtsson et al., 2008).

En annan faktor som påverkar validitet vid just intervjuer i ett forskningsarbete är partiskhet. Partiskhet är en återkommande bov i intervjuer och den främsta förklaringen till detta är att det är mänskligt. Partiskhet kan vara något som är återkommande genom flertal olika intervjuer som en forskare gör, vilket kan leda till att partiskheten är konsekvent och därmed inte upptäcks. Bell (2010) beskriver att det finns många faktorer som kan påverka partiskhet och det kan uppstå både avsiktligt eller i ovetande. Vidare beskriver hon att det är en fälla som forskare lätt trillar ned i, exempelvis vid val av litteratur och källor. Om forskaren enbart väljer ut de källor som talar för samma sak som forskaren själv, är risken stor att en viss partiskhet uppstår (Bell, 2010). Detta stärks även av Berndtsson et al. (2008) som även de beskriver partiskhet som en risk till validitet. Författarna betonar att forskaren bör vara medveten

om att forskningsstudier alltid påverkar en organisation till viss del. När en studie använder sig av flertal intervjuer förklarar författarna att intervjupersonerna ofta kan ändra sina uppfattningar om vissa frågor. Detta kan till exempel bero på att forskaren har utfört sin studie inom deras organisation. Vissa förändringar kan vara svåra att uppfatta, men är en viktig del att uppmärksamma när validitet adresseras. Det blir därmed viktigt att forskaren uppskattar möjligheten för att förhållanden eller situationen kan förändras under studiens gång (Berndtsson et al., 2008). Detta blir en viktig faktor att uppmärksamma under arbetets gång, eftersom studien kommer utföras inom en organisation. Bell (2010) beskriver även vikten av att forskaren håller sig kritisk av de tolkningar som görs av insamlad data och att ta kloka och vaksamma beslut. Hon uppmanar att ofta ifrågasätta utövandet och att när det är möjligt använda triangulering (Bell, 2010). Genom att studien även riktas externt och inkluderar intervjuer med respondenter från andra företag, ger detta upphov till triangulering som kan bidra till att validitet upprätthålls.

4.3 Observationer

Bell (2010) menar att ostrukturerade observationer kan vara ett passande val om forskaren är ute efter att generera en hypotes. Däremot tar det lång tid och kan vara svårt att hantera. Författaren fortsätter med att säga att observationen och den tolkning som görs måste säkerställas; fältanteckningar behöver skrivas ner direkt och den efterföljande tolkningen av dessa anteckningar tar ännu längre tid, samt kräver en viss erfarenhet hos forskaren (Bell, 2010).

I studien kommer direktobservationer göras av ett informationssystem som behandlar personuppgifter. Systemet driftas och förbereds inför GDPR av det IT-konsultföretag som forskaren utför studien på och därmed agerar datakälla åt forskaren. Dessa direktobservationer innebär att forskaren kan observera ett fenomen med egna ögon. Observationen sker på den plats där fenomenet förekommer och forskaren behöver därmed inte förlita sig på sådant som andra berättar. Esaiasson, Gilljam, Oscarsson och Wängnerud (2012) beskriver hur direktobservationer kan vara särskilt bra vid studerande av strukturer eller processer som det kan vara svårt att sätta ord på. De menar att när inblandade parter i ett fenomen är mitt uppe i det som händer kan det bli att de får tunnelseende och inte längre ser allt som pågår (Esaiasson et al., 2012).

Studien kan anses vara en naturalistisk undersökning, i och med att observationerna kommer att kombineras med intervjuer som en ytterligare datainsamlingsmetod. Att kombinera observationer med andra datainsamlingsmetoder är hur naturalistiska undersökningar vanligen bedrivs. Denna typ av undersökning brukar beskrivas att syftet är att söka efter kunskap i sammanhang som är naturliga för de personer, grupper m.m. som observeras (Esaiasson et al., 2012). I och med att observationen ska ske inom ett IT-konsultbolag, där utvecklare arbetar med ett system för att förbereda det inför GDPR, kommer observationen ske i naturliga sammanhang för de involverade personerna och informationssystemet.

Esaiasson et al., (2012) poängterar även att de observationer där forskaren är ute efter att generera en hypotes eller teori, tjänar forskaren på sikt mer genom att hålla en lägre grad av struktur för sin observation. Detta eftersom fler, nya infallsvinklar kan identifieras under undersökning när den är mer öppen och mindre strukturerad. En hårt strukturerad observation passar bättre när en teori redan finns som forskaren ska pröva (Esaiasson et al., 2012). I en öppen observation informeras även de personer som ska ingå i observationen om vilket syftet är (Ahrne & Svensson, 2011). En öppen observation passar studien bra eftersom den inte baseras på en färdigformulerad hypotes som ska testas, utan strävar efter att formulera en teori baserat på resultat och analys.

En nackdel kan dock identifieras för öppna observationer där de människor som ingår i observationen kan påverkas av vad som kallas för "forskareffekt". Detta innebär att vetskapen om att en forskare observerar kan göra att människors beteende ändras. En forskare som kan samspela på ett bra sätt gör dock att detta enklare kan undvikas. Observationer brukar även beskrivas med begreppen delaktig eller passiv (Ahrne & Svensson, 2011) där studiens observation kommer vara en partiellt delaktig observation. Detta för att dels behålla självständighet som forskare, men även eftersom omgivningen inte tillåter fullt deltagande. Forskaren kommer inte ha självständigt tillträde till det system som kommer observeras.

En annan nackdel med observationer är att när det önskas att ta fram information om känslor, handlingar, tolkningar eller intentioner hos människor, kan de vara svåra att använda. Dessa faktorer kan tydligare visa sig under intervjuer (Esaiasson et al., 2012). Genom kombinationen av observationer och intervjuer kan en större bredd ges för den information som samlas in. Observationerna kommer att utföras tills det att ingen ny information väsentlig till själva fenomenet och studiens syfte kommer fram; observationerna avslutas när det finns en teoretisk mättnad (Esaiasson et al., 2012).

5 Resultat

Detta kapitel presenterar empirin från de intervjuer och observationer som gjorts under arbetets gång. Materialet är strukturerat efter arbetets två delfrågor där mönster från intervjuer och observation presenteras. Genomgående kommer pilotintervjun inkluderas i materialpresentationen, då författaren bedömde att den givit ett tillräckligt gediget och informationsrikt underlag. Samtlig information som har samlats in har grovt sorterats efter kategorier. Kategorierna bestämdes utifrån det som konsekvent uppkom under intervjuer och observation. Den information som ej ansågs ha relevans till studiens delfrågor sorterades bort. Information med större relevans till forskningsfråga och delfrågor delades upp utifrån dessa kategorier för att tydligare kunna presentera insamlad data.

5.1 Delfråga 1

”Vilka är de viktigaste kraven inom GDPR för befintliga informationssystem?”

Det första av de två delfrågor som tagits fram bemöttes genom att i intervjuerna be respondenterna berätta om deras GDPR-arbete, hur de anser att arbetet går och vilka utmaningar de anser sig stå inför. Vidare, för att få en bättre bild av de system som används, ställdes mer tekniska frågor om hur de arbetar med olika begrepp och krav som GDPR ställer. De blev även tillfrågade vilken eller vilka de största, tekniska utmaningarna de anser sig ha.

5.1.1 Aktuellt GDPR-arbete och utmaningar

Respondent 1 är studerande för att bli IT-säkerhetstekniker och har tidigare utfört praktik och nu examensarbete på den organisation som är datakälla åt detta arbete. Respondent 1 berättade om sin delaktighet i GDPR-arbetet på organisationen under sin praktik, som även fortsatt under examensarbetet. I organisationen svarade Respondent 1 att e-post är den största utmaningen som identifierades i GDPR-arbetet. Det lyftes hur e-post sedan tidigare inte är något som berörs särskilt mycket i Personuppgiftslagen, utan är något som har gått under Missbruksregeln.

”Det gör ju att vi i Sverige har lite slapp, om man får uttrycka sig så, hantering av e-post och vad man får skicka. Vi tänker oss inte för, för vi har aldrig haft några direktiv eller riktlinjer för vad man ska skicka och på vilket sätt.” – Respondent 1

Respondent 1 poängterade hur e-post inte bara bör ses som en kommunikationskanal, men även informationskanal. Detta eftersom många sparar e-postmeddelanden för att kunna leta information vid senare tillfällen. Respondent 1 menade att e-post fungerar som minnesanteckningar och att en tolkning av den nya lagstiftningen blir att se på e-post som en transport av information. I relation till just e-post tog Respondent 1 upp viss problematik och lyfte frågan hur organisationer ska bära sig åt för att uppfylla GDPR-kravet ”Rätten att bli glömd” i e-post.

”Vad är det för typ av information som ska tas bort? Räcker det med att den personen bara har nämnts i e-post, att man kan koppla det till en person, det är mycket sånt. Sen skickar man ju otroligt mycket Excel-filer till exempel och det kan ju vara all möjlig data i det.”
– Respondent 1

Enligt Respondent 1 krävs det att en struktur behöver finnas för hur informationshantering via e-post ska hanteras för att samtliga ska veta vad de får göra och inte – något som ansågs vara en utmaning i sig att ta fram. I dagsläget anser Respondent 1 ändå att de inom organisationen har bra koll på hur läget ser ut och var information finns. Svaret gavs att om organisationen kommer kontrolleras den 26:e maj finns det underlag att visa upp hur det har arbetats med att vara i linje med lagstiftningen. Det poängterades däremot att detta inte är hållbart på lång sikt. För att uppfylla lagstiftningens krav i framtiden menar Respondent 1 att det krävs automatiserade funktioner och arbetssätt, direktiv och policys, samt utbildning av personal för att klara av att vara i linje långsiktigt.

Pilotrespondenten är arkitekt inom teknisk ledning på företaget där studien utförs. Uppfattningen hos Pilotrespondenten var att det är utmanande att förstå intention och innebörd i GDPR i jämförelse med Personuppgiftslagen. Gällande hur väl organisationen anser sig vara i linje med lagstiftningen menade Pilotrespondenten att de ligger ganska bra till när det gäller nyutvecklade system, om kravet för ”Rätten att bli glömd” inte räknas med. För existerande system upplevdes situationen inte se fullt lika bra ut. Pilotrespondenten beskrev hur många företag idag inte har en klar uppfattning om hur pågående intrång och brott detekteras om inte någon utomstående säger till. Organisationer som inte har förberedelse för att hantera intrång har svårt att få sina informationssystem i linje med GDPR, då de får svårigheter att klara av GDPRs tidslinjer, menade Pilotrespondenten.

Innebörden och intentionen hos lagstiftaren och förordningen sågs som en svårighet även av de andra respondenterna. Respondent 4 är IT- och projektchef på ett företag inom återvinning och avfallshantering. Respondent 4 poängterade att problematiken med att förstå förordningen gav upphov till frågor om vilka praktiska konsekvenser den också medför. Det lyftes att det kan tänkas se olika ut på olika nivåer. Inom organisationen Respondent 4 arbetar på har de upplevt en viss besvärlighet i att kunna sätta nivån för de åtgärder som ska tas. Vidare berättade Respondent 4 att olägenheterna med att kunna förstå lagen och vidta rimliga åtgärder ligger i att det behövs instruktioner och processbeskrivningar. Det upplevdes svårt att hitta en nivå för GDPR på grund av brist på praxis. Det togs även upp att en risk kan finnas i att ett företag spenderar allt för mycket tid, pengar och kraft på något som i slutändan inte gagnar Dataskyddsförordningens syfte – att skydda den personliga integriteten.

”Det är lätt att man vidtar en massa åtgärder för man är orolig för att ha till exempel ett Excel-dokument, så man delete:ar alla Excel-dokument som har namn i sig. Sen inser man att det kanske inte gagnar skyddet av personlig integritet, det enda det gör är att det

försvårar för folk att få tjänsterna utförda, vid kvalitetssäkring eller försvårar service till medarbetare." – Respondent 4

Liknande svar gavs även av Respondent 2, Business Manager Online på ett stort fashionföretag. Respondent 2 svarade att tolkningen av lagen och att förstå lagen är den största utmaningen med GDPR.

"Vi vet ju inte vad som är vad, det är ju problemet, att lagen må vara en gråzon, men när sedan vi eventuellt blir utsatta för någon revision eller liknande, då är det bannemej inte någon gråzon, då är det antingen rätt eller fel. Så vi måste ju försöka förutse vad som kommer att vara lagstiftarens förväntan…" – Respondent 2

Respondent 2 lyfte även att till följd av att den största utmaningen är att förstå intentionen av lagstiftningen, är den andra utmaningen att kunna leva upp till den. Gällande företagets förberedelse inför GDPR ansåg Respondent 2 att de inte kommer klara av att vara helt i linje med förordningen tills det att den träder i kraft, men de har ambition för att göra sitt bästa utifrån den tolkning de gjort av lagstiftningen. Respondent 2 poängterade att det finns många exempel på när deras jurister ändrar åsikt varje dag om hur något ska tolkas. När det inte går att veta exakt vilken tolkning som är korrekt, menade Respondent 2 att det finns stor sannolikhet för att de kan ha chansat fel.

"Vi har jurister över hela Europa och då pratar de med varandra och då kanske en tysk jurist säger en sak ena dagen och så kommer de på något annat en annan dag, då får vi ta hänsyn till det för det är inte så enkelt i dagsläget. Lagstiftningen och lagtexten är tyvärr inte så solklar." – Respondent 2

Vidare tog Respondent 2 även upp att de medvetet kommer avvika från förordningen på ett antal punkter och att de får ta den risken, då de ansåg sig vara tvungna att tänka på vilka affärsmässiga beslut de behöver ta. Det lyftes dock att det inte bara handlar om att vara vinstdrivande, utan att vissa saker i förordningen inte anses vara möjliga.

När det kommer till att vara i linje med GDPR svarade Respondent 4 att de i grunden anser sig ligga ganska bra till. Det lyftes att de kartlagt verksamheten och dess processer, kartlagt vart behandlingar av persondata sker, uppdaterat registerförteckningar med nya uppgifter och gjort riskanalyser på alla punkter och åtgärdsprogram. Dock ifrågasattes det hur mycket som måste åtgärdas och ageras på innan lagen träder i kraft. Respondent 4 menade att uppfattningarna om vad det innebär har varit olika hos dem kontra Göteborgs Stad. Då de är ett kommunalt bolag behöver synpunkter från Göteborgs Stad också beaktas, inklusive idéer från konsulter och dem själva inom verksamheten. Respondent 4 poängterade att de har som mål att samtliga anställda ska kunna känna sig trygga och veta hur de ska hantera personuppgifter i sitt arbete. Det lyftes att de satsar på generella policys som talar om hur verksamheten ser på hantering av personuppgifter och att det ska finnas tillräckliga instruktioner för detta. Genom intern utbildning i vad GDPR är och innebär, menade Respondent 4 att de

försöker komma så nära de kan innebörden av vad det betyder att göra rätt enligt förordningen. I samband med detta har de även valt att ta fram FAQ med frågor kring vad som får skickas och hur, vilka personuppgifter som får stå var m.m.

Även Respondent 5 är applikationsägare, leveransansvarig och support på samma arbetsplats som Pilotrespondenten och Respondent 1. Respondent 5 ansåg att de låg ganska bra till med sitt införande av GDPR i perspektivet av det informationssystem de driftar. Vidare togs det upp att de nått steget för att slutföra en rapport på det arbete de gjort. Denna rapport kommer fungera som en handbok åt slutkunden. Respondent 5 berättade att ett stort GDPR-fokus ligger på att få det informationssystem som de driftar och som forskaren själv observerat, att vara i linje med förordningen. Det lyftes att GDPR-arbetet för systemet började med en GAP-analys för att identifiera funktioner och processer som hade brister. Respondent 5 förklarade att mycket handlade om att förstå vad varje artikel i förordningen innebar i praktiken. Detta kan se annorlunda ut i och med att det är en juridiskt skriven lag, men systemen är tekniska, menade Respondent 5. GAP-analysen resulterade i ungefär hälften tekniska justeringar och hälften organisatoriska processer. Det togs även upp att en större satsning gjordes på de tekniska justeringarna i form av att ta in extra utvecklare. Detta baserades på att utvecklingen av de tekniska funktioner som skulle läggas till var mer tidskrävande än de processer som behövde sättas på plats. Främst såg Respondent 5 en problematik gällande samtycke, vilket beskrivs mer längre ned i kapitel 5.1.2 – De största tekniska utmaningarna.

Medvetenhet kring att inte vara helt i linje med GDPR, som påpekades av Respondent 2, uttrycktes även av Respondent 3. Respondent 3 är CIO för ett investmentbolag. Det förklarades att de under kartläggning och konsekvensbedömning, som gjortas inför start av deras GDPR-arbete, identifierade större och mindre risker där de ansåg att de får ta de mindre riskerna. Respondent 3 menade att de fick prioritera de största kraven och riskerna, men att hålla det öppet att medvetenhet finns för mindre risker som ej bemötts - utifall att Datainspektionen skulle undersöka dem. De större riskerna som Respondent 3 tog upp att de kommer bemöta tas upp längre ned i texten under kapitel 5.1.2.

På samma sätt som Respondent 2 tog upp gråzoner i GDPR, lyfte Respondent 3 att i relation till förståelse för förordningens intention, upplevdes det att flera delar av GDPR blir svåra just på grund av många gråzoner. Ett exempel på en gråzon som Respondent 3 tog upp var vad skriftligt samtycke innebär i förordningen. Respondent 3 menade att skriftligt betydde en sak några år tillbaka, men att samhället idag även beskriver e-post som skriftligt. Det blir då en fråga om politiker bedömer begreppet på samma sätt. Respondent 3 tyckte därmed att ostrukturerad data i form av e-post och hur det ska behandlas som en stor utmaning.

”Samtycke skriftligt, det är en omöjlig situation. Skriftligt för några år sedan var något helt annat än vad det är idag när vi är digitala, när vi digitaliserat allting.”
– Respondent 3

Befintligt skydd av personuppgifter
Samtliga respondenter blev tillfrågade om organisationen de arbetar på i dagsläget redan använder något befintligt skydd av personuppgifter. Denna fråga besvarades genomgående med att ingen lösning var framtagen för att specifikt skydda just personuppgifter. Pilotrespondenten tog däremot upp att de bedriver ett säkert utvecklingsarbete där applikationen som helhet skyddas. Det påpekades att säkerhet är ett ständigt krav och att de därmed också ställer krav på att obehöriga inte ska kunna se särskilda uppgifter. De hade inte sett behov av att göra mer än så, svarade Pilotrespondenten. Respondent 1 tog upp att det kan variera och är upp till de anställda där de, beroende på kompetens, kan ha egna lösningar för att skydda personinformation. Respondent 1 trodde detta kan bero på en avsaknad av riktlinjer.

Exempel på existerande skydd som mer generellt används hos de olika respondenterna, var bland annat kryptering av lösenord och personnummer i system. Respondent 2 berättade även hur de använder sig av behörighetskrav för att skydda vem som har tillgång till vilken information. Vidare svarade Respondent 2 att de arbetar enligt ISO 27001 och PCI DSS som standarder för att skydda finans- eller betalinformation och att det är mycket säkrat. Respondent 3 tog istället upp avtal som en form av skydd där de inför GDPR tagit fram avtal gällande just personinformation som deras leverantörer behöver skriva på. Respondent 4 lyfte hur de hittills använt sig av en PuL-policy som kommer ersättas av en GDPR-policy för hur personuppgifter ska skyddas. Utöver det tog Respondent 4 även upp att de arbetar med behörighetshantering vilket inkluderar personuppgifter utöver annan information i verksamheten.

5.1.2 Tekniska utmaningar och uppfyllande av GDPR:s krav

Pseudonymisering
Begreppet pseudonymisering hade de flesta respondenter först kommit i kontakt med genom förordningen. Ett par av respondenterna hade arbetat med begreppet till viss del, bland annat i relation till Personuppgiftslagen. Pilotrespondenten berättade att det i informationssystemet som ingår i detta arbetes observationer används en algoritm ovanpå personnummer för att pseudonymisera denna data. Vidare lyftes även Google Analytics som ett exempel där en viss pseudonymisering sker genom att unika användare kan identifieras utan att IP eller användarnamn är synligt. På så vis går det inte att säga vem som står för trafiken.

Pseudonymisering är enligt Respondent 2 den största, tekniska utmaningen inom GDPR som företaget står inför. Det påpekades att det generellt sett finns en önskan om att kunna identifiera en person i de flesta typer av system. Detta väcker frågan hur någon identifieras som inte ska identifieras, menade Respondent 2. Svaret gavs att fullständig pseudonymisering inte är möjligt hos dem i deras organisation. Det lyftes då att de inte vet något företag som kan erbjuda anonymiserad data som innehåller den informationsmängd som de kräver.

”I vissa fall är det alltså inte ens tekniskt möjligt. Hur ska man kunna anonymisera en person i alla system och ändå kunna ta bort all information om den personen - hur gör man det?” – Respondent 2

För organisationen Respondent 2 arbetar på vill de veta information i form av kunders köpbeteende. Både till marknadsföring, men även för logistik. För detta menar Respondent 2 att de i sådana fall skulle behöva anonyma data som ser precis ut som verkligheten och som beskriver verkligheten, men utan att vara baserad på verkligheten. Det är av denna anledning som de anser att de inte kan ligga på full anonymitet eller full pseudonymisering.

”När vi pratar utveckling och test kan man fråga varför vi vill veta dessa sakerna, när det gäller BI och AI då är det ju självklart, men när blir det viktigt för utveckling och test? Jo vi vill ju skapa system som har rätt ’performance’, rätt användarvänlighet och så vidare och det kan vi bara göra genom att titta på verkligheten.” – Respondent 2

Pseudonymisering berättade Respondent 3 att de valt att använda i de fall där radering av data inte kunde ske i ett system. Respondent 3 förklarade att de väljer att skriva över den information som blir kvar med exempelvis XXX för att ta bort möjligheten att kunna se informationen. Respondent 4 berättade att de också använder sig av en form av pseudonymisering och att de gjort detta sedan tidigare. I flera fall har de GPS-system som följer deras fordon och för detta anges ett fordonsnummer istället för att individer ska följas på personnummer. När de sedan tittar på informationen från ett systemperspektiv är den pseudonymiserad. Det lyftes dock att det inte finns många ställen inom verksamheten där pseudonymisering skulle vara intressant eller tillämpningsbart. Detta berodde på att de har personuppgifter på uppdrag av kommuner och därmed har laglig grund genom kommunallagen, förklarade Respondent 4.

Inom det system som författaren observerat berättade både Pilotrespondenten och Respondent 5 att det sedan tidigare finns en algoritm på personnummer som ändras till en annan slumpmässig kombination av siffror. Detta berättade Respondent 5 är något som generellt används inom bilbranschen och kallas för ”bilägarnummer” och skulle kunna ses som en form av pseudonymisering. Eftersom denna funktionalitet redan fanns på plats sedan tidigare, menade Respondent 5 att det inte fanns någon problematik kopplad till den delen av GDPR. Vidare tog Respondent 5 även upp att de tillämpar anonymisering vid de tillfällen någon vill bli glömd, där de tar bort informationen och låter fältet vara tomt.

Dataportabilitet

Gällande kravet för Dataportabilitet beskrev Pilotrespondenten detta som något omöjligt att genomföra ur en teknisk synvinkeln, om det inte ges exakt information för vart data ska flyttas. Om Dataportabilitet är något som berörs inom organisationen var Pilotrespondentens spontana tanke att det i sådana fall sker manuellt och för hand. Däremot ansågs det finnas utrymme för att möjliggöra åt en kund som eventuellt skulle vilja flytta data. En del av organisationens produkter har en del liknande funktionalitet,

men att möjliggöra för en kund att flytta data till en konkurrent är det sista organisationens kunder önskar göra, svarade Pilotrespondenten.

Respondent 2 nämnde hur kravet för Dataportabilitet skapat problematik för dem. Det poängterade att det finns en svårighet för dem att kunna avgöra vart gränsen går för vad de förväntas berätta för en kund, och vad som är deras affärshemligheter i relation till rättigheten hos individen. Respondent 2 fortsätta även med att berätta att Dataportabilitet kan tänkas ge upphov till missbruk av kriminella eller även intresseorganisationer. Det skapar en möjlighet för kriminella att använda sig av utpressning, eller av intresseorganisationer att använda det som påtrycksmedel i försök att skada företaget, menade Respondent 2. Detta potentiella missbruk lyftes därmed som en tredje, stor utmaning som ansågs betungande för företaget.

Vidare tog Respondent 2 också upp att Dataportabilitet är besvärligt i bemärkelsen att det är krångligt att genomföra i praktiken. Respondent 2 ifrågasatte hur själva flytten skulle ske om en kund begär ut sin data, samt aspekten att informationen enligt lag även ska vara tolkningsbar. Som exempel berättade Respondent 2 att de lagrar enorma mängder av sin information på engelska och en fråga blev då om de ska översätta all information i sådana fall. Fortsättningsvis berättade Respondent 2 att de valt att bemöta problematiken genom att skapa ett formulär på engelska som innehåller den information som de tillhandahåller. Detta formulär följs sedan av ett följebrev där det kommer skrivas ut vad för information det är som finns. Följebrevet kommer sedan stå på det språk som gäller för postadressen dit informationen ska skickas.

Respondent 3 lyfte Dataportabiliteten som den del av förordningen de verkligen inte förstår sig på. Däremot påpekade Respondent 3 att det är ett krav som inte ansågs beröra dem, då de inte använder sig av system där Dataportabilitet skulle bli relevant. Samma sak gällde även enligt Respondent 5 som påpekade hur Dataportabilitetskravet blev irrelevant för det driftade informationssystemet. Detta berodde på att privatpersoner inte har egna konton i systemet och därmed inte kan lägga upp något som skulle kunna flyttas över till en annan leverantör.

Respondent 4 berättade att Dataportabilitet är något de arbetar med och har gjort sedan tidigare. Dock påpekades det att det inte sker i det syftet som GDPR avser, där en individ önskar byta leverantör. Respondent 4 berättade att Dataportabilitet hos dem innebär att de får uppdrag av en kommun på mellan 5 och 7 år. Därefter kan kommunen välja att byta leverantör och de måste då lämna ifrån sig alla adressuppgifter, vilka tjänster som är knutna till varje adress, samt vem som är skriven på adressen för att nästkommande leverantör ska veta vem som ska faktureras. Respondent 4 förklarade att det inte händer ofta, men att de är duktiga på att plocka ut information och kunna lämna ifrån sig data till andra leverantörer när det behövs. För enskilda individer var dock inte Dataportabilitet lika relevant. Detta förklarades med att de aldrig fått en sådan förfrågan från en privatperson, samt inte förväntade sig denna typ av förfrågan i framtiden.

Rätt till radering – ”Rätten att bli glömd” och loggning
Kravet för ”Rätten att bli glömd” var återkommande hos en majoritet av respondenterna. Pilotrespondenten upplevde att det är funktionaliteten för att uppfylla ’Rätten att bli glömd’ som är det tekniskt mest utmanade. Respondent 1 påpekade hur GDPR upplevs som svårtolkad och att många diskussioner på organisationen har varit kring just hur data ska raderas. Det togs upp att det finns en svårighet i att veta vilken information det är som ska raderas i bland annat e-post, om en person ringer om ber om att bli bortglömd.

Respondent 3 förklarade hur det ansågs vara en omöjlighet att uppfylla ’Rätten att bli glömd’ i alla system på grund av saknat stöd i CRM-system. Respondent 3 berättade att de sett hur vissa CRM-system de använder inte har stöd för att kunna radera data och att de därmed inte kan uppfylla kravet för ”Rätten att bli glömd”. Det påpekades även att det är svårt för dem att påverka vad system kan och inte kan göra när de själva inte äger ERP-systemen som finns kopplade. För att bemöta denna utmaning berättade Respondent 3 att de valt att lösa problematiken med pseudonymisering istället. I de system där data inte kan raderas kommer de istället pseudonymisera och skriva över informationen för att ta bort möjligheten att se eller spåra den, förklarade Respondent 3.

Genomgående hos respondenterna uttrycktes det att ”Rätten att bli glömd” även är ett svårt krav att bemöta gällande loggning. Pilotrespondenten berättade att de använder sig av Azure Application Insights och Amazon AWS X-Ray för loggning då dessa produkter har lagringsfunktionalitet. Det förklarades att data ligger kvar under en begränsad tid för att sedan raderas per automatik. Fortsättningsvis tog Pilotrespondenten upp ’Rätten att bli glömd’ som ett exempel och förklarade att om en kund skulle ringa in till dem och be om att bli raderad blir det svårt att hantera i loggarna. Hittills har detta lösts genom att bemöta en sådan förfrågan med funktionen ’Drop Database’ över den period som data om kunden finns med. För att glömma bort en kund i loggarna behövs alltså alla loggar tas bort i och Pilotrespondenten kommenterade att produkterna de använder kräver funktionalitet för att kunna ta bort enskilda individer. Det påpekades av Pilotrespondenten att det finns många tekniska produkter som används för loggning och att det blir upp till leverantören att vara i linje med GDPR.

Respondent 2 uttryckte att i och med att GDPR ställer högre krav på loggning, skapar det större svårigheter än vad de anser sig kunna hantera inom företaget. Respondent 2 berättade att de loggar stora mängder information och att de även loggar saker då det finns lagkrav att de måste göra det. Respondent 2 förklarade att det inte är något konstigt med att de loggar stora mängder information. Till stor del beror det på att de dagligen utsätts för många olika typer av attacker och försök till missbruk. Orsaken till att de loggar den mängd information som de gör, är för att kunna hitta bedrägligt beteende och för detta måste loggar finnas för alla personer. Respondent 2 lyfte problematiken att GDPR är otydlig för hur radering praktiskt ska bemötas, eftersom informationen måste sparas en viss tid. För att bemöta denna problematik förklarade Respondent 2 att de valt att skilja på ’Retention time’ och ’Residence time’. De har angett

en viss 'Residence time' för data och att det finns ett syfte med den tiden. Denna 'Residence time' behöver även vara så kort som behövs för att utföra syftet med lagringen. I och med detta väljer de därmed att ha kvar sina loggar även om en kund ber om att bli raderad. Loggarna finns dock enbart kvar under precis den tid som syftet kräver. Respondent 2 påpekade även att kunderna trots detta ska kunna känna sig trygga i att deras loggar är skyddade av behörighetskrav.

"Vi kommer vara tydliga i kommunikationen tillbaka till kunden, vilket vi har skyldighet att vara, att vi har viss information kvar och vi har den på grund av det som är vårt syfte. Det är så vi hanterar loggar, men det är ett stort problem." – Respondent 2

Respondent 3 berättade att de internt inte ansåg sig veta alla loggar och allt som loggas i deras system. Däremot påpekades det att det är svårt för dem att kunna hantera loggar då leverantörerna säger att det ligger på leverantörerna själva att sköta det. När de själva tittat i sina system menar Respondent 3 att det oftast inte är personinformation som finns i systemen, men de hade hittat IP-adresser som sparats i systemen. Trots att detta enligt GDPR är en personuppgift, förklarade Respondent 3 att de själva inte kan identifiera någon på en IP-adress och de har därför bedömt att intern information i loggar inte berörs av GDPR.

Respondent 4 förklarade att de främst loggar vid behov. Det viktigaste är de centrala systemen som har någon form av juridisk funktion, såsom ekonomisystem. I loggarna kan personuppgifter förekomma, men loggning av system sker är inte ämnat för personuppgifter. Kravet för att en individ ska kunna bli bortglömd och få sin information raderad var inte ett bekymmer hos Respondent 4. Detta beror på att verksamheten Respondent 4 arbetar på har kommunallagen i ryggen. I och med att de är ett kommunalt bolag bedrivs verksamheten på uppdrag av kommuner. Respondent 4 förklarade att detta innebär att de har laglig grund till all behandling av individers personuppgifter. Vidare förklarades det även att information inte kan raderas i deras arkiv eftersom de följer arkivlagen och räknas som en myndighet i det avseendet. Verksamheten får därmed inte lov att göra sig av med uppgifter på grund av att de har en skyldighet att arkivera handlingar och uppgifter som upprättas, berättade Respondent 4.

Backuphantering

Under intervjun togs även backuphantering upp där respondenterna fick berätta hur detta används inom deras arbetsplats. Pilotrespondenten lyfte backuphantering som den andra, största, tekniska utmaningen och förklarade att det fanns en osäkerhet för hur backuphanteringen på organisationen går till. Däremot påpekades det att den information som har högst värde att backa upp inom organisationen är användarinformation. Respondent 1 svarade att backup finns för alla servrar och att backup ligger 5–7 dagar bakåt i tiden.

Respondent 5 förklarade att de använder sig av en driftleverantör för det informationssystem som observerats i studien. Det är hos leverantören som servrarna körs och det finns även produktionsmiljö och testmiljö. Respondent 5 berättade att de har köpt tjänster att drifta och ta backup på systemet där de kan gå 12 månader tillbaka i tiden. Utöver detta sker det daglig backup och inkrementellt varje timme i produktionsmiljön. Den backup som görs är av både databasen och applikationsdata. Denna backup togs dock inte upp som någon problematik, Respondent 5 nämnde att det ansågs viktigast att prioritera det som har störst påverkan på individers integritet.

”Det ska väl en hel del till att någon stjäl ett backup-band och hittar en person - i så fall är det ju kris för alla berörda som ligger i den backupen, inte bara de som är glömda.”
– Respondent 5

Respondent 2 tog upp att det inom företaget händer mycket hela tiden och att de därför har kort livslängd på sina backuper. I relation till ’Rätten att bli glömd’ och GDPR menade Respondent 2 att det inte blir en problematik i backup om en kund ringer och ber om att bli bortglömd. Informationen kommer redan ha raderats och backupen ersatt av en ny version, förklarade Respondent 2.

Respondent 3 berättade att de istället ligger på backup i trettio dagar och anser sig därmed att vara i linje med GDPR i och med att en person kommer vara borta helt och hållet efter den tiden. Det poängterades dock att de upplevde backuper som en ytterligare gråzon, då den data som ligger på backup är i molnet och inte kan nås digitalt eller av dem själva. Vidare trodde Respondent 3 att backup kan bli ett större problem längre fram om de börjar spara års-backuper, men att de får bemöta den frågan först då.

Respondent 4 förklarade att de använder två sätt att arbeta med backup. Dels backar de på databasnivå upp de centrala ekonomi- och ERP-systemen. Dessa är speglade och fysiskt separerade. All annan information ligger i ett SAN som backas upp på olika sätt beroende på verksamhetens krav. De kan ta snapshots vid olika tidsintervall och tar full backup på nästan all information en gång i veckan. I koppling till GDPR lyfte Respondent 4 ingen problematik gällande backupen.

Respondent 5 påpekade en viss problematik för ’Rätten att bli glömd’ i koppling till backup. Det togs upp att de rent tekniskt inte kan gå in och redigera backup-band för det observerade systemet. Istället har de valt att skapa en lista över de personer som har raderats från systemet. Varje person sedan tidigare tilldelats en sträng med en slumpmässig kombination av bokstäver och siffror. Detta används sedan för att identifiera om en ”glömd” person finns med i backupen, så att de efter en återläsning kan raderas på nytt, berättade Respondent 5.

De största tekniska utmaningarna

Utöver de tidigare nämnda utmaningarna ’Rätten att bli glömd’ och backuphantering som ansågs vara de största tekniska utmaningarna enligt Pilotrespondenten, samt fullständig pseudonymisering som var utmanande enligt Respondent 2, togs ytterligare en del utmaningar upp av de andra respondenterna. Enligt Respondent 4 ansågs det istället vara verksamhetens generella dataskydd. Det påpekades att det kanske inte var i direkt koppling till GDPR, men då GDPR innebär ett större ansvar för att skydda personuppgifter blir det allt mer relevant att tänka på verksamhetens informationssäkerhet och IT-säkerhet generellt. Respondent 4 tog upp skydd mot risk för intrång och ransomware som exempel på sådant som blir viktigare att jobba med. Enligt Respondent 5 är den största tekniska utmaningen att kunna hitta logik för att praktiskt kunna bemöta de krav GDPR ställer på dataminimering, samt att begränsa tiden som data sparas i ett system. Respondent 5 påpekade att utöver att det varit svårt att hitta logiken, även har varit svårt att ha kraft i systemet för att kunna ställa den typen av frågor som krävs för att bemöta dessa krav.

Respondent 5 ansåg också att det fanns stora svårigheter rörande samtycke och laglig grund för det informationssystem som organisationen driftar. Då det handlar om ett system i fordonsbranschen där slutkunden inte har tillgång till systemet på samma sätt som andra system, kan det bli både enklare och svårare, menade Respondent 5. Det lyftes att slutkunden inte är den som loggar in i systemet och bidrar med information. Istället handlar det om återförsäljare som lägger in information där det mesta kommer från kontrakt mellan köparen och generalagenten. Respondent 5 menade att det då inte var helt klart om samtycket för lagringen av personuppgifterna behöver fångas upp på samma sätt som för att personuppgifter ska få finnas i systemet. Det blir svårt att veta hur samtycket ska se ut i systemet. Hittills har de byggt en checkbox för samtycke av datalagring i systemet där det blir upp till säljaren att bocka i den checkboxen, berättade Respondent 5. De har även lagt till en checkbox i koppling till att en potentiell kund vill boka testkörning och personer samtycker då till lagring av personuppgifter för att uppfylla syftet. Huruvida samtycket sedan ska in och visas i systemet upplevs desto svårare. Respondent 5 påpekade hur det kan tyckas vara enkelt i själva förordningen, men blir tekniskt utmanande.

Respondent 3 lyfte att det ansågs tekniskt utmanande att många system behöver byggas om. Det påpekades att detta blir en dyr process som istället kan resultera i mycket manuellt arbete då funktionaliteten saknas i systemen. Respondent 1 upplevde istället att det mest utmanande är att hitta de rätta, tekniska lösningarna till förordningens krav och att kunna implementera ett fungerande uppföljningsarbete. Det togs även upp att det finns en utmaning i att bemöta ’Rätten att bli glömd’ i koppling till e-post. Som ett exempel nämndes även samtycke i koppling till ’Rätten att bli glömd’. Respondent 1 svarade att en stor utmaning inom just e-post och samtycke är de CV:n som skickas in och sparas och att det blir en fråga om hur samtycke i en sådan situation ser ut.

Observation – tekniska utmaningar
Observation av det befintliga informationssystemet på det företag där författaren utfört studien, skedde i förberedelsefasen för att sortera ut data som inte längre behövdes. Detta gjordes för att minimera mängden data som fanns registrerad i informationssystemet och bemöta dataminimeringen inom GDPR. Onödiga data som det inte fanns syfte eller laglig grund för att spara identifierades för att sedan kunna rensas bort från systemet. För framtida rensning av personuppgifter krävdes det även att ett beslut skulle fattas gällande 'Retention time'. Detta innebar att en tid behövde anges för under hur länge personuppgifter skulle få lov att finnas kvar i systemet. Denna 'Retention time' skulle även vara olika beroende på vilken typ av kund det handlade om; om det gällde en person som slutkunden skrivit ett kontrakt med, eller en individ som endast gjort en provkörning. I koppling till denna 'Retention time' blir en kund inaktiv efter en viss tid om ingen ändring har gjorts för kunden i systemet. Detta kunde vara i form av offert, modifiering i databasen eller liknande. Efter att en kund har klassats som inaktiv kommer den raderas ur systemet.

I koppling till dataminimering kunde viss svårighet gällande 'Rätten att bli glömd' identifieras under arbetets gång. För att vederlägga hur radering skulle bemötas i informationssystemet, både i bemötande av dataminimering och Rätten att bli glömd, sågs data över för att se vilken data som pekade på en identifierbar person och kunde kopplas till identifieringstecken. Data som därmed kommer att raderas för att bemöta denna rätt hos individen gäller exempelvis adress, adresshistorik, e-postadress, namn och telefonnummer, personnummer, kundnummer och kopplade aktiviteter såsom provkörning. De fält vars data ska raderas blir istället tomma fält, med undantag för data som ej kan raderas på grund av laglig grund i form av nationell lag, policys eller direktiv. Data som bevaras i systemet kunde därmed ej vara identifierande eller erhålla någon koppling till annan data i systemet som kan härledas och identifiera en person.

För att arbeta fram funktionaliteten i systemet för att radera de kunder som inte längre skulle finnas kvar i systemet behövde vissa fel åtgärdas. En del kunder i systemet visade sig kunna vara unika för vilka kopplingar de hade i systemet. Där fanns kunder med fler och mer djupgående kopplingar mellan data och vissa kunder kunde därmed ha fler kopplingar till identifierande fält. Exempel på ett fel som åtgärdades hittades vid test av raderingen i produktionsmiljön. Det kunde ses att vissa kunder hade fler relaterade tabeller i databasen med identifierande fält som trots radering inte rensats.

Vid senare observation skulle funktionen för att radera lagrade kunder testas. Det första steget innebar att säkra en backup av databasen för att kunna hämta tillbaka raderade data. Detta följdes av steg nummer två vilket var att genomföra raderingen. Totalt omfattande raderingen runt två miljoner kunder som påträffats genom uppfyllande av dataminimering. Detta test möjliggjorde för identifiering av relationer mellan tabeller för att kunna se om där fanns en kvarvarande problematik. Det möjliggjorde även för att kunna se om någon data kvarstod och om där fortfarande fanns personuppgifter kvar. På grund av mängden data visade sig raderingen ta för lång tid att genomföra. Ett sätt

för att portionera ut rensningen vid olika tillfällen behövde därmed hittas genom att avgöra en gräns för hur stor mängd data som kunde raderas åt gången. Det fanns då åter igen en svårighet i att vissa kunder hade data kopplad till många olika delar i systemet.

I informationssystemet gjordes även ytterligare åtgärder i form av en tillagd säkerhetsfunktion som kräver att användare uppdaterar sitt lösenord var 90:e dag. Tillhörande ges även information och riktlinjer för hur ett säkert lösenord bör se ut. Denna typ av säkerhetsaspekt saknades sedan tidigare i informationssystemet. Vidare lades funktionalitet till för att kryptera den kundinformation som skickas till extern kund som hanterar marknadsföring. Tidigare låg denna information helt öppet.

5.2 Delfråga 2

"Hur väl går de sju grundläggande principerna inom Privacy by Design att uppfylla för befintliga informationssystem?"

Den andra delfrågan för att hjälpa besvara arbetets frågeställning bemöttes genom att i intervjuerna fråga respondenterna om de kunde berätta hur de varit i kontakt med begreppet Privacy by Design. Vidare togs det också upp om de kände igen att de arbetade efter någon eller några av de sju grundläggande principerna. Samtliga respondenter blev tillfrågade om de sedan tidigare var bekanta med begreppet Privacy by Design där en tydlig majoritet först hade kommit i kontakt med metoden i samband med GDPR. För att ta reda på om de redan arbetade enligt de grundläggande principerna, fick samtliga respondenter ett informationsblad som kort beskrev innebörden av varje princip.

5.2.1 Pilotrespondent

Pilotrespondenten kunde identifiera alla principerna inom sin organisation och lyfte särskilt *'Proactive not Reactive; Preventative not Remedial'*. Det påpekades att deras utvecklingsarbete är proaktivt när det gäller säkerhet i allmänhet, inklusive inbrottssäkerhet. I och med ett proaktivt arbete tog Pilotrespondenten även upp att de uppfyller *'Privacy Embedded into Design'*. Pilotrespondenten svarade att deras användare inte ska behöva göra någonting gällande säkerhet själva och att de därmed följer principen "*Privacy as the Default*". '*Full Functionality – Positive-Sum, not Zero-sum*' ansågs vara ett konstigt krav att ställa då det ansågs vara en självklarhet i att integritet och säkerhet inte ska ställas mot varandra. Pilotrespondenten menade att begreppen alltid ska finnas tillsammans och att organisationen därmed arbetade med den principen också. Vidare berättade Pilotrespondenten att de även uppfyller *'End to End Lifecycle Protection'* och *'Respect for User Privacy'*. Den princip som det potentiellt kunde finnas avsaknad på var *'Visibility and Transparency'*, då Pilotrespondenten förklarade att de inte tydliggjort att det är Privacy by Design de följer, utan att de istället ställer säkerhet som ett krav.

"Jag antar att det handlar om att Privacy by Design är tydliggjord i processerna och inte bara i tekniken." - Pilotrespondent

5.2.2 Respondent 1

Respondent tyckte sig inte ha tillräckligt med kunskap om organisationen och dess arbetssätt och avstod från att svara. Det ansågs att svaret som bäst skulle kunna vara spekulativt då Respondent 1 inte tyckte sig vara i en position att kunna besvara frågan.

5.2.3 Respondent 2

Respondent 2 berättade att de inom företaget aktivt arbetar med Privacy by Design, men påpekade att det som de sju grundläggande principerna beskriver är självklarheter och att motsatsen till principerna skulle vara onaturligt för dem. Samtliga av principerna följs då de sågs som sunt förnuft och inte som något nytt, enligt Respondent 2. Vidare gavs ett exempel på vad de faktiskt tillfört som något nytt i företaget utifrån Privacy by Design och hur de väljer att tolka innebörden av metoden. Respondent 2 förklarade då att de arbetar med att göra det enkelt för sina utvecklare att förstå både GDPR och Privacy by Design. De har därför förändrat sin utvecklingsmetodik och dokumentering för att göra det enklare för sina utvecklare att förstå hur de praktiskt ska arbeta för att hålla kundens integritet i åtanke hela tiden. De har även valt att lägga till checkpunkter som kollas av mot sina utvecklare för att göra det lättare för utvecklare och testare att följa.

”Privacy by Design är att kunder, anställdas, personers integritet ska man ha i åtanke när man är arkitekt, när man utvecklare, testare eller vad man än är. Så medvetenhet och utbildning är väldigt viktigt.” – Respondent 2

5.2.4 Respondent 3

Respondent 3 påpekade hur Privacy by Design är något de kommer hålla i åtanke och ändra sin utveckling efter, men att det blir enklare att implementera vid nyutveckling. Den största problematiken ligger i gamla system där det är flera saker som blir svåra att uppfylla, förklarade Respondent 3. Det lyftes också hur principen *’Privacy Embedded into Design*’ kan vara problematiskt vid inköp av molnlösningar, då det redan finns en färdig design utvecklad innan GDPR som kan vara svår att ändra. Fortsättningsvis togs det upp hur många ERP-system är felbyggda från början och därmed har svårt att leva upp till principerna i och med att samma krav inte ställdes när de utvecklades. Däremot identifierade Respondent 3 att principerna *’End to End Lifecycle Protection’* och ‘*Respect for User Privacy*’ var sådant som återfinns inom organisationen.

”Det blir lättare om det ska designas ett nytt system, men alla har inte råd att göra det.”
- Respondent 3

5.2.5 Respondent 4

Respondent 4 uppgav att de inte börjat bemöta Privacy by Design tillräckligt genomgående inom verksamheten ännu. De kommer ta med Privacy by Design utifrån vad GDPR säger i verksamhetens policys kring hur de kommer bedriva sitt förbättringsarbete för deras system, berättade Respondent 4. De kommer även att ta

hänsyn till Privacy by Design vid upphandlingar som en form av underlag. Respondent 4 förklarade att de inte gått in mer i detalj på vad Privacy by Design praktiskt kommer innebära, utan de har valt att bemöta den frågan längre fram. Vidare påpekade Respondent 4 att det behövs funktionalitet för att bemöta GDPR och Privacy by Design praktiskt i systemen. Det upplevdes att det troligen skulle bli enklare för alla om det finns en unison bild genom standardisering och automatisering av hur det ska gå till. Respondent 4 tog även upp att huvudsyftet med förordningen inte får glömmas av och menade att eftersom GDPR och Privacy by Design handlar om den personliga integriteten är det viktigare att större kraft läggs på större företag som löper större risker gällande personlig integritet. Exempel på företag som nämndes var då Facebook, Google och Spotify, kontra de mindre system som används på arbetsplatsen för Respondent 4.

"Vad det gäller den personliga integriteten som ju är huvudsyftet i det här, så är det ju oerhört mycket större risker och mycket viktigare att Google och Facebook och Spotify och de här, jobbar med dessa frågorna, än att vårt vågsystem ska göra det. I och med att riskerna är otroligt små i ett sådant system, så det är helt olika dimensioner på vad det innebär. " – Respondent 4

5.2.6 Respondent 5

Respondent 5 svarade utifrån det informationssystem som studiens observation gjorts på. Principen *'Proactive not Reactive; Preventative not Remedial'* ansågs uppfyllas genom den algoritm som sedan tidigare fanns i systemet där personnummer omvandlas vad som kallas för "bilägarnummer". *'Privacy as Default'* trodde Respondent 5 att det dock inte fanns mycket av i just det systemet. Det påpekades att Privacy är en del inom färdigifyllda alternativ och checkboxar. Respondent 5 menade på att det är sunt förnuft att respektera användaren och inte välja saker åt individen. Under förberedelsearbetet av system inför GDPR har de därmed haft detta i åtanke. Gällande principen *'Privacy Embedded into Design*' ansåg Respondent 5 att det skulle kunna se bättre ut. Däremot togs det upp att de i systemet inte representerar kunder med huvudnyckel. Istället använder de sig av en unik identifierare som tilldelas varje kund och denna är i sin tur kopplad till alla metatabeller. Detta innebär att personuppgifterna försvinner på samtliga ställen, trots att det endast behöver rensas på ett ställe. *'Full Functionality – Positive-Sum, not Zero-Sum*' kändes inte igen och Respondent 5 ansåg att det var svårt att svara ja eller nej på om den principen finns med i systemet. Vidare tryckte Respondent 5 på vikten av principen *'End-to-End Lifecycle Protection'* och menade att säkerheten inte bara ska finnas när ett system utvecklas, utan att system även ska avvecklas på ett säkert sätt. Denna princip ansågs alltid varit "best practise", även innan integriteten kom in i bilden, och att principen funnits med av informationssäkerhetskäl. Principen *'Visibility and Transparency'* påpekade Respondent 5 att det var något som kan förbättras. Detta berodde på att det fanns en svårighet att kunna vara helt transparent och öppen med vilken data som läggs in i systemet. Anledningen bakom svårigheten, som tidigare nämnt, var att det är säljare ute i själva bilhallen som lägger in data i

systemet och att mycket hänger på bilföretagets instruktioner. Däremot tog Respondent 5 upp att det är tydligt i själva köpeavtalet att det samlas in integritetsinformation och vad den används till. Vidare upplevde Respondent 5 även att principen *'Respect for User Privacy'* som något mycket viktigt att tänka på, särskilt ur ett support-perspektiv. Respondent 5 förklarade att det är något som alltid tas hänsyn till genom att ifrågasätta hur saker skickas och hanteras, av respekt för slutkunden. Däremot görs detta mer i processer än inom systemprogrammering för Respondent 5 del.

6 Analys

Detta kapitel presenterar resultatet av den analys som gjorts av den insamlade empirin. Kapitlet är uppdelat utefter studiens delfrågor. Analysen kommer lyfta de mönster och kontrast som kan ses insamlat material i jämförelse med den litteratur som har använts. Analysen har strukturerats upp utefter relevanta kategorier för att bidra till en tydligare presentation av de fynd som gjorts. Analysens första steg bestod av att ställa respondentsvar i studiens resultat mot varandra. Detta gjordes för att identifiera mönster för likheter och olikheter i svar relaterade till studiens två delfrågor. Identifierade mönster i resultatet ställdes sedan mot det resultat som tagits fram utifrån studiens observation för att se om samma mönster återfanns även där. Resultat från intervjuer och observation ställdes sedan mot förordningstexten och de krav som identifierats. Vidare gjordes även en jämförelse mot källor i studiens bakgrund. Detta för att ta reda på huruvida studiens resultat talade för samma sak som berörs i litteraturen. Detta inkluderade även källor som berörde Privacy by Design och dess sju grundläggande principer. Analysen beskriver studiens resultat i form av grova kategorier som representerar de mönster som identifierats i relation till förordningstexten och ytterligare källor. Analysen ger grunden som studiens slutsats och checklista baseras på, vilket beskrivs i kapitel 7.2.

6.1 Vilka är de viktigaste kraven inom GDPR för befintliga informationssystem?

Genomgående hos respondenterna uttrycktes svårigheten med att förstå innebörden och intentionen i förordningstexten. Detta påverkade i sin tur att det fanns en osäkerhet för hur krav inom GDPR bör bemötas rent praktiskt – både ur ett tekniskt och organisatoriskt perspektiv.

Rätten att bli glömd

Uppfattningen om ’Rätten att bli glömd’ ansågs vara en stor utmaning enligt samtliga respondenter. Då många av respondenterna arbetar med informationssystem med relationsdatabaser påpekades det hur radering i vissa system ansågs tekniskt omöjligt. Att kunna radera kunddata upplevdes också särskilt svårt i relation till loggning, då flera respondenter uppgav att de rent praktiskt inte hade någon långsiktig lösning på hur det ska hanteras. I förordningstexten beskrivs detta krav under Artikel 17 och innebörden är att en individ har rätt att be personuppgiftsansvarig, det vill säga de som hanterar personuppgifterna, att radera individens uppgifter. Denna förfrågan måste genomföras om de som behandlar personuppgifterna ej har laglig grund att behålla dem, om behandlingen av personuppgifterna krävs för utövning av yttrande- och informationsfriheten, om behandling görs inom området för folkhälsa eller för arkivändamål (Europaparlamentets och rådets förordning (EU) 2016/679). Respondent 4 arbetar för ett kommunalt bolag och påpekade att detta medför att de följer kommunallagen, samt arkivlagen vilket ger dem laglig grund att behålla och behandla de personuppgifter de hanterar.

Pilotrespondenten berättade hur de inom organisationen i nuvarande situation upplevde hur en stor del av kravet för ’Rätten att bli glömd’ var i koppling till loggar och åtminstone ett systems databas. Pilotrespondenten tog då upp att hela databasen måste tömmas för att möjliggöra för radering av enbart en person. Saknas syfte eller laglig grund måste de genomföra förfrågan av radering. En avsaknad av funktionalitet för radering av sådan skala skapar problematik rent tekniskt och kan tänkas gälla för flera företag.

Respondent 1 nämnde ‘Rätten att bli glömd’ i koppling till hur detta krav bör appliceras för ostrukturerad data i form av e-post. Det ansågs att det kan bli svårt att uppfylla detta krav inom e-post, eftersom det är en välanvänd kommunikationskanal där stora mängder information sparas. GDPR ger en tydlig förklaring för vad som anses vara en personuppgift, där även ostrukturerad data kommer ingå efter att missbruksregeln försvinner i samband med GDPR. Huruvida lagen kommer följas korrekt inom e-post ansåg Respondent 1 hängde på tydliga policys inom organisationen. Organisationer och myndigheter förväntas att inför att GDPR träder i kraft, ge dokumentation för hur de är i linje med förordningen. Artikel 24 i förordningstexten beskriver hur organisationers ansvar innebär att de kan påvisa att förordningen följs. Detta inkluderar även att införa både organisatoriska och tekniska åtgärder för att säkerställa att förordningen följs (Europaparlamentets och rådets förordning (EU) 2016/679). Detta skulle exempelvis kunna vara en policy med riktlinjer över arbetet eller certifikat.

Rätten att bli glömd är även en av de faktorer som Tikkinen-Piri, Rohunen och Markkula (2018) identifierade som de mest väsentliga implikationer som GDPR för med sig. Lämpliga processer och säkerhetsåtgärder bör därför finnas på plats för att möjliggöra för radering av personuppgifter i informationssystemen. Författarna tog upp vikten av dokumentation i relation till uppfyllandet av detta krav där det bör presenteras hur data lagras och om data delas med tredjeparts (Tikkinen-Piri, Rohunen & Markkula, 2018). ’Rätten att bli glömd’ är komplext vilket leder till att organisationer måste se över den påverkan kravet ställer på en detaljerad nivå. Det blir av stor vikt att överväga påverkan på befintlig teknologi och därmed inkludera faktorer såsom omfång, kostnad och möjlighet.

Samtycke

Lagligt samtycke beskrivs i Artikel 7 i förordningstexten med tillhörande ’Skäl 32’. Det framgår även i Artikel 4, punkt 11 att definitionen av samtycke bland annat kan ske genom en tydlig och bekräftande handling (Europaparlamentets och rådets förordning (EU) 2016/679). Respondent 1 tog upp samtyckesfrågan i relation till e-post. Det ifrågasattes hur samtycket ska se ut och hur det ska inhämtas. Som exempel nämndes CV som skickas till företag och sedan sparas hos exempelvis rekryterare. Det kan då kan bli problematiskt att avgöra om det finns ett tydligt samtycke eller inte, menade Respondent 1. Det kan tänkas att ett frivilligt skickat e-postmeddelande för att ge ett CV till ett företag, kan anses vara en tillräckligt bekräftande och tydlig handling som i sig innebär ett givet samtycke.

Respondent 5 lyfte hur samtycke var en problematik i det informationssystem som studiens observation gjorts på. Det togs upp att det fanns svårighet i hur samtycket skulle presenteras och föras in rent tekniskt i informationssystemet. Detta berodde på att informationssystemet används inom fordonsbranschen av de säljare som sitter i bilhallar. Det blir då upp till säljaren att samla in samtycket för lagringen av personuppgifter. Detta kan ske skriftligt eller muntligt och hur detta sedan översätts in i informationssystemet upplevde Respondent 5 som en utmaning. En tanke fanns kring att i informationssystemet lägga till möjligheten att fylla i om samtycke från en kund finns eller inte. I och med att samtycket är inhämtat av säljaren, kan det tänkas att information och riktlinjer bör finnas på plats för säljaren för vad som ska skrivas in i systemet. Exempelvis att säljare efter ett skrivet kontrakt även anger i informationssystemet att det finns givet samtycke. Artikel 7 i förordningstexten beskriver villkoren gällande samtycke. Där framgår det att den personuppgiftsansvarige som behandlar personuppgifterna måste uppvisa samtycke från individen vars personuppgifter behandlas. Ges samtycket i samband med andra frågor, ska samtycket tydligt kunna urskiljas (Europaparlamentets och rådets förordning (EU) 2016/679). Det skulle kunna tänkas bli en fråga i fallet för Respondent 5, om det skriftliga samtycket på ett kontrakt mellan en kund och bilsäljare anses vara nog, eller om tydlighet för samtycke måste presenteras även i informationssystemet.

Samtycke är en av de faktorer av implikationer med GDPR som Tikkinen-Piri, Rohunen och Markkula (2018) tog fram. Författarna identifierade en potentiell utmaning med samtycke i relation till att det kan innebära ett behov av ytterligare resurser. De tog även upp att det kan leda till en kostnadsfråga i form av exempelvis implementation av ett separat system för att hantera samtycke. De bemötte även att det alternativt kan innebära nya processer för att samla in samtycke eller registrera tillbakadragande av samtycke (Tikkinen-Piri, Rohunen & Markkula, 2018)

Dataportabilitet

Kravet för dataportabilitet beskrivs i Artikel 20. Kravet innebär att GDPR ger varje EU-medborgare rätten att få den information de givit till ett företag flyttad till en annan tjänst. Detta ska antingen ske direkt från en tjänst till en annan där det är tekniskt möjligt. Alternativt ska det vara möjligt för individen att få ut data på ett strukturerat, maskinläsbart format som vanligen används och därefter kunna skicka data vidare till en ny tjänst (Europaparlamentets och rådets förordning (EU) 2016/679).

Flera av respondenterna uttryckte en problematik kring dataportabilitet och såg det som en stor utmaning att uppfylla i sina system. Genomgående påpekades det även av respondenterna att de inte ansåg Dataportabiliteten som ett uppskattat krav inom förordningen. Pilotrespondenten lyfte exempelvis fram att det sista deras kunder vill möjliggöra för, är att någon ska kunna byta och flytta sin data till en konkurrent. Detta uppmärksammandes av Respondent 2 och 3 likaså.

Skulle det visa sig omöjligt att genomföra en direkt överföring av data från en tjänst till en annan, bemöter lagen detta och det bör då istället vara möjligt att skicka data till den

individ som begär ut den istället. Detta skulle då kunna tänkas vara ett sätt att bemöta potentiell problematik för Pilotrespondenten. Däremot påpekade Respondent 2 hur kravet för Dataportabilitet anses ge upphov till eventuellt missbruk där företag kan ta skada om de förväntas lämna ut information som anses vara affärshemligheter. Artikel 15 i GDPR beskriver 'Rätten till information' som kan tänkas tydligare beröra det som Respondent 2 lyfte som en farhåga i form av missbruk. Rätten till information innebär att en individ har rätt att begära information om ett företag behandlar deras personuppgifter och vilka personuppgifter det är som behandlas. Inkluderat i denna information är syftet med behandlingen, vilka kategorier av personuppgifter det gäller, mottagare av informationen och under vilken tidsomfattning behandling och lagring sker. Det ska även ges information om varifrån personuppgifterna kommer om de ej inhämtats från individen i fråga, samt om det sker profilering eller annat automatiserat beslutsfattande. Individen ska även få information om dess rätt till radering, rättelse eller begränsning av behandlingen, samt rätten att klaga till en tillsynsmyndighet (Europaparlamentets och rådets förordning (EU) 2016/679).

Dataportabilitet lyftes av Tikkinen-Piri, Rohunen och Markkula (2018) som en av de mest väsentliga faktorerna inom förordningen. De förklarar i sin studie att organisationer kommer förväntas ha implementerat processer som möjliggör för en flytt av personuppgifter om en sådan förfrågan görs. För detta bör organisationer se över i vilket format data kommer skickas. Det bör även ses över om funktionalitet finns för direkt överföring av personuppgifter från ett informationssystem till ett annat. Författarna poängterade att avsaknaden av standard för hur överföringen ska ske kan innebära en utmaning för organisationer (Tikkinen-Piri, Rohunen & Markkula, 2018). I likhet till detta lyfte även Respondent 4 att avsaknad av standarder och praxis gör förordningen svårt att följa i praktiken, exempelvis implementering av tekniska åtgärder.

Pseudonymisering

I förordningstexten GDPR tas pseudonymisering upp som en potentiell skyddsåtgärd. Organisationer rekommenderas använda dessa åtgärder för att säkerställa en nivå av skydd av personuppgifter. Skäl 78 beskriver att lämpliga tekniska och organisatioriska åtgärder ska implementeras och tar upp pseudonymisering som en åtgärd som bör göras omgående (Europaparlamentets och rådets förordning (EU) 2016/679). Utifrån respondenterna var det enbart Respondent 2 som uttryckte en omöjlighet gällande fullständig pseudonymisering inom deras företag. Respondent 2 förklarade att detta berodde på att de kräver data med stor informationsmängd för marknadsföring och logistik. Respondent 2 berättade att de måste därmed använda data som är baserad på verkligheten. Av denna anledning krävs det att de bevarar data för att kunna genomföra exempelvis sin marknadsföring som baseras på kunders köpbeteenden. Ett annat exempel som Respondent 2 tog upp var möjligheten att kunna vidareutveckla tillräckligt användarvänliga system och till det behövs data som är baserad på verkligheten. Övriga respondenter uppgav inte pseudonymisering som ett problem hos dem. Istället beskrevs

det som ett medel att kunna bemöta kravet för 'Rätten att bli glömd', i viss likhet med förordningstexten.

Anmälan av personuppgiftsincident

GDPR beskriver en personuppgiftsincident som ett säkerhetsbrott som leder till att personuppgifter förloras, förstörs, förändras eller blir tillgängliga till obehöriga (Europaparlamentets och rådets förordning (EU) 2016/679). Artikel 33 i förordningstexten berör den anmälan som måste göras om en personuppgiftsincident inträffar. Denna anmälan ska ske inom 72 timmar från det att vetskap finns om incidenten. Den som tar emot anmälan är den behöriga tillsynsmyndigheten och försening av anmälan måste kunna motiveras (Europaparlamentets och rådets förordning (EU) 2016/679). Pilotrespondenten tog upp hur det upplevdes en avsaknad att kunna detektera säkerhetsbrott, såsom exempelvis stöld av data. Ofta krävs en utomstående som kan identifiera om dataintrång har skett och att det finns en problematik i koppling till anmälan om personuppgiftsincident, menade Pilotrespondenten. Det skulle kunna tänkas att en svårighet i att detektera säkerhetsbrott eventuellt leder till att kravet för att anmäla en personuppgiftsincident ej uppfylls på ett tillfredsställande vis enligt förordningen. Tikkinen-Piri, Rohunen och Markkula (2018) lyfte också hantering av personuppgiftsincident som en väsentlig faktor att beakta i GDPR. De tog upp att organisationer bör etablera processer som på ett tydligt sätt möjliggör för att ett snabbt agerande sker i det fall att en personuppgiftsincident skulle inträffa. Vidare poängterades det att, utöver tillsynsmyndigheten, ska den individ som en incident berör också kunna informeras skyndsamt. För att säkerställa att detta kan ske bör det kontrolleras hur de personer vars data en organisation behandlar, kontaktas på snabbast möjliga sätt (Tikkinen-Piri, Rohunen & Markkula, 2018). Skulle avsaknad av lämpliga tekniska säkerhetsåtgärder finnas för de personuppgifter en incident gäller, ska individen ej kontaktas angående incidenten. Detta eftersom det eventuellt kan innebära en större risk för individens personuppgifter om information kring en incident ges till individen utan att säkerhetsåtgärder finns på plats. För att möjliggöra att information om en personuppgiftsincident ska kunna skickas tas kryptering upp som ett exempel på en rekommenderad åtgärd i Artikel 34 i förordningstexten (Europaparlamentets och rådets förordning (EU) 2016/679). Eventuellt kan vissa säkerhetsåtgärder innebära större förändringar i funktionaliteten i organisationers informationssystem.

Inbyggt dataskydd och dataskydd som standard

Kravet för 'Inbyggt dataskydd och dataskydd som standard' förklaras i Artikel 25 i GDPR och är mycket relevant till metoden Privacy by Design. Innebörden av kravet är att det ska finnas inbyggt dataskydd, både inom system och organisation, genom hela behandlingsprocessen av persondata. I artikeln tas dataminimering och Pseudonymisering upp som exempel på åtgärder, men artikeln specificerar ej exakta åtgärder som måste göras. Det är upp till organisationerna och myndigheterna själva att hitta de mest lämpliga lösningarna (Europaparlamentets och rådets förordning (EU) 2016/679). Eventuellt skulle en organisation som implementerat lösningar utefter de

sju grundläggande principerna inom metoden Privacy by Design kunna uppvisa att detta krav därmed uppfylls. Vikten av detta krav lyftes även av Tikkinen-Piri, Rohunen och Markkula (2018) som poängterar att organisationer bör säkerställa att de har policys som stödjer en proaktiv implementation av säkerhetsåtgärderna för att uppfylla detta krav. De tog även upp funktionalitet för dataminimering som en sådan åtgärd. Detta menade de kan möjliggöra för organisationer att kunna se till att enbart ett minimum av den data som krävs behandlas. Fortsättningsvis skulle implementering av dataminimering även vara ett sätt att säkra att personuppgifter inte sparas längre än det behövs (Tikkinen-Piri, Rohunen & Markkula, 2018).

6.2 Hur väl går de sju grundläggande principerna inom Privacy by Design att uppfylla för befintliga informationssystem?

För att besvara delfråga nummer två analyserades de olika intervjurespondenternas svar mot varandra. Detta gjordes för att se om någon av de sju grundläggande principerna inom Privacy by Design återkom oftare. Vidare ingick det även i analysen att sedan ställa svaren från intervjuerna mot det som hade identifierats under observationerna. Detta för att identifiera likheter och olikheter. Analysen bestod även av att ställa fynden i form av likheter och olikheter mot tidigare använda dokument och källor angående GDPR och Privacy by Design.

Huruvida intervjurespondenterna upplevde att någon eller några av principerna inom Privacy by Design tillämpades inom deras organisation, visade sig se olika ut för de olika respondenterna. Det lyftes av flera respondenter att Privacy by Design är något som enklare tillämpas på nyutveckling. Respondent 3 påpekade hur det kan vara problematiskt att rusta upp äldre system utefter Privacy by Design. Detta eftersom äldre system skapades och designades i en tid då integritet inte var en lika stor fråga, menade Respondent 3. På grund av avsaknad av stöd i flera ERP-system ansågs det att det var svårt att uppfylla flera av principerna. Däremot identifierades *'End to End Lifecycle Protection*' och '*Respect for User Privacy*' att användas inom organisationen. Gällande *'End to End Lifecycle Protection*' upplevde Respondent 3 hur det i många fall troligen är enklare att byta system när de äldre systemen inte går att åtgärda. Det kan tänkas att denna princip därmed blir extra relevant om vissa system inte kan vara i linje med GDPR och behöver avvecklas. Respondent 5 lyfte också *'End to End Lifecycle Protection'* och påpekade att detta är något som även utan integritetsfrågan har ansetts som 'best practise' inom arbetsplatsen.

Cavoukian (2010) beskriver att hennes metod Privacy by Design fordrar att integriteten byggs direkt in i det organisatoriska och tekniska inom ett företag. Hon liknar Privacy by Design som det nästa steget inom dialogen om säkerhet (Cavoukian, 2010). I linje med detta påpekade Pilotrespondenten hur mycket av det säkerhetsarbete de redan bedriver idag täcker stora delar av Privacy by Design. Detta skulle då kunna tänkas tyda på att ett

gediget säkerhetsarbete kan uppfylla flera av principerna enbart genom sitt fokus på säkerhetsaspekten i hela organisationen. Pilotrespondenten och Respondent 2 var de som ansåg sig arbeta efter samtliga principer. Pilotrespondenten upplevde däremot att särskild dokumentation för att påvisa att det arbetas enligt Privacy by Design i organisationen skulle kunna vara något att tillföra. Respondent 2 uttryckte istället de sju grundläggande principerna som sunt förnuft och att de aktivt arbetar med metoden.

Principen *'Full Functionality – Positive-Sum, not Zero-Sum*' upplevdes svår att besvara enligt Respondent 5. En viss osäkerhet påpekades även av Pilotrespondenten. Enligt Cavoukian (2010) har de senare åren präglats av ett paradigm där två värden ställs mot varandra och bara det ena värdet kan vinna. Hon tar upp integritet som ett värde som ofta har ställts mot exempelvis säkerhet. Hon nämner som ett exempel att många väljer att ge upp integriteten för att ha tillräcklig säkerhet och skydd mot hot såsom terrorism. Hon menar att detta tankesätt kommer från falsk dikotomi och att begreppen integritet och säkerhet ska bemötas ömsesidigt (Cavoukian, 2010). Detta påpekades även av Pilotrespondenten som uttryckte att det inte är rätt att ställa integritet och säkerhet mot varandra, då de är sammanhängande begrepp. Tankesättet om att säkerheten och integritet hör ihop fanns även hos Respondent 2.

Respondent 5 tog upp att *'Privacy as Default'* troligen inte uppfylldes till fullo för just det informationssystem som studien observerat. Cavoukian (2010) tar upp att denna princip uppfylls genom funktionalitet som innebär att användaren själv inte ska behöva utföra något för att skydda sin egen integritet, istället ska sådana åtgärder redan finnas inbyggda i systemet (Cavoukian, 2010). Respondent påpekade däremot att de under förberedelsearbetet haft integritet i åtanke vid utveckling av ny funktionalitet. Däribland implementerades checkboxar för samtycke som ej redan är ifyllda åt kunden i förväg. Utöver detta togs det upp att kundinformation för marknadsföring numera krypteras, till skillnad från tidigare.

Respondent 5 tog även upp att *'Privacy Embedded into Design'* skulle kunna bemötas bättre, och Respondent 3 påpekade svårighet för principen i relation till molnlösningar. Cavoukian (2010) anser att denna princip innebär att integritet ska vara en komponent inom funktionaliteten för exempelvis ett informationssystem. I och med detta ska integritet inte vara något som byggs på i efterhand, utan finns inbäddat från början (Cavoukian, 2010). Flera av respondenterna ansåg att Privacy by Design kan vara svårt att uppfylla för gamla system och eventuellt bidrar denna princip mer till denna problematik. Detta eftersom integritet kan ses som något som byggs på i efterhand på äldre system för att vara i linje med förordningen GDPR.

Respondent 5 uppgav att det inom det observerade informationssystemet kan förbättras för principen *'Visibility and Transparency*'. Enligt Cavoukian (2010) innebär denna princip att affärspraxis och teknologi ska fungera enligt de löften och mål som sats upp inom en organisation. Detta ska framföras tydligt och transparent mot leverantörer, användare och andra intressenter (Cavoukian, 2010). Respondent 5 ansåg att öppenhet

fanns, men att det handlar mycket om det säljare som arbetar ute i bilhallarna säger till kunderna och vilken data de registrerar i systemet. Det påpekades att det ligger på det bilföretag som är slutkunden för informationssystemet att instruera sina säljare om öppenhet och transparens.

7 Slutsats

7.1 Besvarande av forskningsfråga

Detta kapitel avser summera det svar som kan ges till studiens forskningsfråga som är följande:

"Hur påverkas befintliga IT-system av GDPR och Privacy by Design och hur kan en checklista användas för att avgöra hur redo ett system är för GDPR?"

Studiens analys identifierade mönster för vilka krav inom GDPR som det enligt respondenter och observerat informationssystem upplevdes utmaningar kring. Analysen tog även fram huruvida de sju grundläggande principerna återfanns inom organisation och informationssystem eller inte. Slutsatsen sammanfattar det som kommit fram ur resultat och analys utifrån de delfrågor som studien har arbetat efter att ge svar på. Studiens forskningsfråga ställdes för att ta reda på huruvida befintliga informationssystem blir påverkade av de krav dataskyddsförordningen GDPR ställer. Då studien även hållit ett fokus på metoden Privacy by Design i koppling till förordningen, har det även undersökts hur väl de sju grundläggande principerna går att tillämpa på befintliga informationssystem. Studiens forskningsfråga besvaras därmed genom de två delfrågorna.

"Vilka är de viktigaste kraven inom GDPR för befintliga informationssystem?"
Vissa krav ur förordningen visade sig vara mer eller mindre appliceringsbara beroende på organisationen det gäller. Krav som har identifierats som väsentliga för vissa informationssystem inom vissa organisationer, har uppfattats som mindre viktiga hos andra respondenter. Ett exempel på detta är dataportabilitet som av ett par respondenter ej ansågs vara applicerbart på deras organisation. På det företag Respondent 2 arbetar på förklarades det att dataportabiliteten kan innebära att de även måste lämna ifrån sin information som räknas som affärshemligheter. Flera respondenter påpekade även olusten i att möjliggöra för kunder att byta till en potentiell konkurrent genom dataportabilitet. Vidare kunde även rekommendationen att använda pseudonymisering som en säkerhetsåtgärd bemötas olika beroende på verksamheten, dock var det en åtgärd som i någon form tillämpats enligt samtliga respondenter.

Trots att utmaningar och svårigheter visade sig se olika ut för olika organisationer och informationssystem, fanns där likväl gemensamma faktorer hos flera av respondenterna. Likhet mellan intervjuer och observation kunde också ses för vilka krav som påverkade informationssystem mer och upplevdes som mest krångliga.
De främsta kraven ur GDPR som studien identifierade som påverkar befintliga informationssystem är följande:

- ***Rätt till radering – "Rätten att bli bortglömd"*** [Artikel 17]
- ***Villkor för samtycke*** [Artikel 7, Skäl 32, Artikel 4]
- ***Rätt till Dataportabilitet*** [Artikel 20]
- ***Rekommendation av pseudonymisering*** [Skäl 78]

- ***Anmälan om personuppgiftsincident*** [Artikel 33]
- ***Inbyggt dataskydd och dataskydd som standard*** [Artikel 25]

"Hur väl går de sju grundläggande principerna inom Privacy by Design att uppfylla för befintliga informationssystem?"

Metoden Privacy by Design hade majoriteten av intervjurespondenterna kommit i kontakt med via GDPR:s krav 'Inbyggt dataskydd och dataskydd som standard'.
Det kunde konstateras att några av de sju grundläggande principerna var mer eller mindre förekommande. De principer som det identifierades en avsaknad på eller som respondenter upplevde kunde förbättras är följande:

- ***Proactive*** *not Reactive;* ***Preventative*** *not Remedial*
  Majoriteten av respondenterna ansåg sig följa denna princip, dock visade sig en avsaknad hos Respondent 3 som ej nämnde att principen uppfylls.

- *Privacy as the* ***Default***
  Även denna princip kunde identifieras att den uppfylls hos flera av respondenterna. Det lyftes dock av Respondent 5 att denna princip troligen inte uppfylls till fullo i det informationssystem författaren observerat i studien.

- *Privacy* ***Embedded*** *into Design*
  Gällande denna princip upplevde Respondent 5 att det kunde bemötas bättre. Det påpekades även av Respondent 3 att principen kan tänkas skapa utmaningar i koppling till molnlösningar där det blir svårt att ändra designen.

- *Full Functionality —* ***Positive-Sum****, not Zero-Sum*
  Respondent 5 var den respondent som ansåg denna princip svår att kunna besvara med ett konkret ja eller nej för om principen uppfylls. Pilotrespondenten uppmärksammande att det upplevdes att principen följs, men att det fanns en viss osäkerhet. Det poängterades att det upplevdes udda att ställa integritet och säkerhet mot varandra, istället bör dessa begrepp samspela.

- ***Visibility*** *and* ***Transparency***
  Respondent 5 och Respondent 3 uppvisade att denna princip inte följdes fullt ut. Respondent 5 ansåg att det kunde förbättras då det fanns en osäkerhet om öppenheten fanns med hela vägen för det observerade informationssystemet. Respondent 3 tog ej upp att denna princip följdes.

För principerna '*End-to-End Security —* ***Full Lifecycle Protection'*** och ***'Respect*** *for User Privacy*' var samtliga respondenter eniga om vikten av att dessa uppfylls och ingen respondent lyfte att det fanns en avsaknad av dessa. Respondent 5 lyfte hur bägge dessa principer alltid måste finnas med och att det är något som upplevdes ha funnits redan innan det blev en fråga om integritet.

7.2 Checklista

Den checklista som var studiens förväntade resultat skapades baserat på studiens analys och slutsats. Checklistan har strukturerats utefter de krav och principer som besvarat studiens två delfrågor. Utifrån detta har åtgärder tagits fram för de mest väsentliga kraven och rekommendationer för samtliga grundprinciper. Del 1 av checklistan bemöter de krav som identifierades som de mest väsentliga för informationssystem att besitta funktionalitet för och utgår därmed utifrån Delfråga 1. Checklistan täcker därmed hur dessa krav i GDPR kan bemötas. Till varje identifierat krav ges svarsalternativ som presenteras i tre nivåer av mognad där Steg 3 är som mest i linje med förordningen. Dessa svarsalternativ togs fram utifrån studiens analys där respondenternas svar ställdes mot varandra för att identifiera mönster gällande aktuellt GDPR-arbete, befintliga säkerhetsåtgärder, samt tekniska utmaningar. Respondenternas svar ställdes även mot relevanta delar inom förordningstexten som berörde de identifierade kraven. Detta låg i grund för att ta fram rekommenderade åtgärder i linje med GDPR. Jämförelse gjordes även mot litteraturen i studiens bakgrund för att ta fram ytterligare lämpliga åtgärder i checklistans svarsalternativ. Steg 1 har därmed baserats på aktuellt GDPR-arbete enligt studiens respondenter i koppling till förordningstextens krav och representerar ett minimum. Steg 2 och 3 beskriver mer detaljerade åtgärder för ett långsiktigt uppfyllande av GDPR som bygger på Steg 1.

Del 2 av checklistan berör istället Delfråga 2 och de sju grundläggande principerna inom Privacy by Design. Samtliga principer har inkluderats baserat på författarens anseende om att principerna går hand i hand och kompletterar varandra. Valet gjordes också utifrån studiens resultat som talade för att uppfyllande av de sju grundläggande principerna inom Privacy by Design kan variera beroende på vilken typ av verksamhet eller vad för informationssystem det gäller. Utifrån respondenternas svar, förordningstexten, samt studiens bakgrund och Dr. Ann Cavoukians definitioner av grundprinciperna, formulerades relevanta rekommendationer att tillämpa på organisation och teknik. Genom dessa rekommendationer bemöter checklistan därmed hur de sju grundläggande principerna inom Privacy by Design bättre kan uppfyllas. Studiens checklista skiljer sig därmed från en checklista Datainspektionen (2018) tagit fram som gäller GDPR. Detta i och med att studiens checklista är baserad på studiens egna empiri, samt inkluderar fokus på Privacy by Design. Genom att arbeta utefter de sju grundläggande principerna inom Privacy by Design anses det även att kravet ”Inbyggt dataskydd och dataskydd som standard” inom GDPR också bemöts i del 2 av checklistan.

Checklistans mognadssteg och rekommendationer innebär implementering av ett systematiskt informationssäkerhetsarbete som inkluderar att åtgärder implementeras för teknik, men även för organisatoriska processer, policys och riktlinjer; fysiska utrymmen och design, samt nätverksarkitektur.

Del 1: GDPR

Rätt till radering **”Rätten att bli glömd”**	**”Hur länge sparas persondata i informationssystem, backup och loggar?”**
	Steg 1: Det har identifierats vilken typ av data som lagras och hanteras i organisationen och personuppgifter har klassificerats. Dataminimering har tillämpats där data som saknar syfte, laglig grund eller samtycke har tagits bort. Det finns policys och förteckningar över hur radering ska ske, samt över de personuppgifter som finns och hur de används. Data behandlas enbart inom en tidsram det finns syfte och/eller laglig grund för. Manuell radering av personuppgift kan ske vid förfrågan. Etablerad kontakt till tredjeparts för information om eventuell radering finns (vid behov). **Steg 2**: Inkluderar Steg 1. Det finns funktionalitet i informationssystem för borttagning av persondata. Backup och loggar rensas inom 30 dagar. **Steg 3**: Inkluderar Steg 1 & 2. Funktionalitet för radering i backup och loggar som innehåller personuppgifter, som sker direkt har implementerats. Det finns implementerat stödjande informationssystem eller stödjande funktionalitet för att hantera förfrågan om radering från individer (vid behov). Dokumentation över radering finns för att snabbt ta bort tidigare raderade uppgifter efter eventuell återläsning av data från tidigare backup.
Villkor för samtycke	**”Hur inhämtas samtycke?”**

	Steg 1: Lagligt samtycke hämtas in där laglig grund ej finns. Om samtycke ges i samband med andra frågor, särskiljs samtycket tydligt åt och urskiljs från övriga frågor eller information, såsom användarvillkor. Samtycket ges fritt från den individ det berör och det går att uppvisa om samtycke är tillbakadraget. Inkluderat finns även information om hur och varför data används, exempelvis om det delas med tredjeparts. Det ges tydlig, transparent information om vad individers val innebär i relation till behandling av personuppgifter. Det ges även information om att samtycke kan dras tillbaka och samtycket undviks att användas som ett förvillkor för bruk av en tjänst. **Steg 2**: Inkluderar Steg 1. Det finns implementerade processer för att kunna uppvisa att samtycke har samlats in från de vars personuppgifter behandlas. Processer och funktionalitet för att verifiera en persons ålder finns implementerat och hänsyn tas till den åldersgräns som gäller för behandling av personuppgifter (minimum 13 år). Vid behov finns funktionalitet för inhämtning av förälders samtycke. Det används inga förvalda alternativ som måste avmarkeras av individer. **Steg 3**: Inkluderar Steg 1 & 2. Det har implementerats funktionalitet i informationssystem, eller implementerats stödjande informationssystem som behandlar inhämtning och tillbakadragning av samtycke.

Rätt till dataportabilitet	**“Hur hanteras dataportabilitet?”**
	Steg 1: Det har identifierats om funktionalitet för direkt överföring av data är möjligt. Det finns kunskap för hur en förfrågan om flytt av data ser ut, samt när det ska genomföras eller när en förfrågan kan nekas. Processer har fastställts för i vilket maskinläsbart och strukturerat format data ska skickas till individer som begär flytt. Processerna inkluderar även tydliga riktlinjer för hur flytten ska ske utan förhinder eller försening. Dataportabiliteten sker genom att data manuellt skickas till den individ som begärt ut den.

	Steg 2: Inkluderar Steg 1. Där det är tekniskt möjligt, finns funktionalitet för att flytta data direkt till en annan tjänst implementerat. Inför eventuell verbal förfrågan om flytt, finns riktlinjer inom policys för hur detta ska registreras. **Steg 3**: Inkluderar Steg 1 & 2. Hänsyn tas till potentiell integritetsrisk vid överföring. En riskbedömning har gjorts och identifierade risker inkluderas i intern utbildning för hur dessa ska bemötas. Säkerhetsåtgärder för att skydda data under överföring, såsom kryptering och antivirusprogram, finns implementerat. Funktionalitet för att sammanställa vilken data som dataportabilitet berör finns implementerat.
Anmälan av personuppgiftsincident	**"Hur bemöts en personuppgiftsincident?"**
	Steg 1: Vid upptäckt av en personuppgiftsincident skickas en anmälan till tillsynsmyndigheten inom 72 timmar. Processer finns på plats för hur en anmälan ska gå till samt för hur en försening av anmälan ska bemötas. Detta inkluderar att ta reda på konsekvenser och begränsningar som en incident kan medföra, samt beskaffenhet av brottet – dessa processer görs inom 72 timmar. **Steg 2**: Inkluderar Steg 1. Mekanismer, funktionalitet eller användande av tjänster finns på plats för att enklare detektera säkerhetsbrott i informationssystem. Nyckelpersoner för samtliga processer involverade i en eventuell personuppgiftsincident är identifierade. **Steg 3**: Inkluderar Steg 1 & 2. Det finns automatiserad funktionalitet implementerat för att skicka en anmälan till tillsynsmyndigheten vid upptäckt av personuppgiftsincident. Det finns säkerhetsåtgärder i form av exempelvis kryptering för att informera den individ en incident berör. Samtliga anställda är utbildade att kunna identifiera potentiella säkerhetsbrott och det finns automatiserade funktionalitet för återställning av data.

Del 2: Privacy by Design

Proactive not Reactive; Preventative not Remedial	Organisationen arbetar proaktivt genom att implementera ett systematiskt informationssäkerhetsarbete som förutser och förhindrar säkerhetsbrott. Inkluderat i detta arbete finns policys, standarder och riktlinjer för hur risker undgås. Informationssäkerhetsarbetet inkluderar även processer i form av riskanalys för både organisation, fysiska utrymmen, nätverksarkitektur och teknik. Säkerhetsåtgärder för att bemöta eventuella brott, såsom kryptering och anonymisering finns implementerat.
Privacy as the Default	Högsta graden av integritetsskydd faktoriseras in inom både organisation och system genom anpassade funktioner, mekanismer eller processer. Individers integritet skyddas genom att behörighet krävs för att se och hantera persondata. Systemkod granskas med jämna mellanrum för att garantera att där inte finns eventuella hål som kan utnyttjas i form av integritetsbrott och säkerhetsbrott. Organisationens praxis och rutiner är formulerat på ett sådant sätt att personuppgifter automatiskt alltid skyddas. Mängden data som lagras och hanteras är minimerad inom system och organisation, samt tillämpas behörighetskrav för personinformation. Transaktioner och interaktioner är som standard ej identifierbara till en specifik användare.
Privacy Embedded into Design	Både organisatoriskt och tekniskt bäddas integritet in i utveckling och design-stadiet, genom hela livscykeln, samt under tiden en användare använder exempelvis en tjänst eller ett system, men även efter att en användare inte längre brukar en applikation eller tjänst. Detta kan ske genom att tidigt tillämpa pseudonymisering eller anonymisering av persondata i system, kryptera personuppgifter och inloggningsuppgifter utefter behov, samt kryptera persondata om den ska skickas. För att utesluta potentiella risker kan ramverket PIA (Privacy Impact Assessment), framtaget av ICO (Information Commissioner's Office) tillämpas för att bidra till att formulera informationsflödet i organisationen, samt för att identifiera risker och åtgärder.

Full Functionality — Positive-Sum, not Zero-Sum	Implementerat finns ett systematiskt informationssäkerhetsarbete enligt standarder ISO/IEC 27001 och 27002. Integritet och säkerhet används tillsammans i organisationen och därmed görs inga kompromisser där integritet ställs mot andra värden. Organisationen håller en balans mellan integritet och affärsintressen och integritetsaspekten försvagar ej funktionalitet. Detta görs genom tydlig dokumentation över organisationens mål och önskade funktionalitet. Säkerhetsåtgärder tas fram för att möjliggöra för multifunktionalitet.
End-to-End Security — Full Lifecycle Protection	Integritetsaspekten är inkluderad vid hela livscykeln för ett system. Persondata skyddas från det att det hämtas in, under bearbetning, lagring och behandling, samt vid avveckling av system. Data raderas på ett säkert sätt som ser till att syftet slutförs. Exempelvis kan skydd finnas för att undvika risk för dataläckage eller stöld av data i samband med att ett system avvecklas. Säkerhetsåtgärderna bör även inkludera stark kryptering och behörighetskontroll, samt säkra metoder för loggning.
Visibility and Transparency	Det finns inkluderat i affärspraxis och policys att öppenhet finns kring hur integritetsfrågan bemöts. Hur funktioner och komponenter fungerar och används är synligt för samtliga inblandade parter, såsom leverantörer och användare. Det finns transparent dokumentation över vilka integritetspolicys som används och detta är tillgängligt för användare.
Respect for User Privacy	Användarens integritet respekteras genom att system är uppbyggda av användarvänliga alternativ och lämpligt beaktande av integriteten. Organisation och utveckling består av standarder för att skydda integriteten. För att uppfylla detta hålls personuppgifter aktuella och korrekta. Användare måste aktivt själva ”opt-in”, dvs. användarna själva fyller i kryssrutor då dessa inte är förvalda. Inhämtning av samtycke görs separat för olika typer av behandling och skiljs åt från användarvillkor. Tydlig information ges för syfte, omfattning, möjlighet att dra tillbaka samtycke, samt om personuppgifter delas med ytterligare parter.

8 Diskussion

8.1 Metodval

Ambitionen för antalet intervjuer var att utföra minst sju till åtta intervjuer för att bättre garantera validitet och reliabilitet. Studien resulterade i ungefär det tidigare tänkta antalet, nämligen sex intervjuer medräknat pilotintervjun. Ett större antal intervjuer hade potentiellt kunnat ökat validiteten och reliabiliteten av resultatet, då mönster i insamlade data troligen hade synts bättre om mängden varit större. Antalet intervjuer kan eventuellt ha påverkat att mjukare slutsatser har dragits utifrån det respondenterna svarat. Dock bör det påpekas att intervjusvaren även ställdes mot insamlade data från observation. Detta för att bättre kunna avgöra om en generalisering kan dras eller inte. Vidare bör det också poängteras att de intervjuer som gjordes anses ha varit bra och gynnsamma då mycket informationsrik data har samlas in.

Det bör uppmärksammas att författaren sedan tidigare hade begränsad erfarenhet av att utföra intervjuer. Intervjuerna under studiens gång ses som en nyttig läroprocess. Den begränsade erfarenheten kan tänkas ha bidragit till att enstaka följdfrågor har formulerats i form av mer stängda frågor. Eventuellt kan enstaka frågor även formulerats ledande utan författarens avsikt. Trots begränsad erfarenhet anses intervjuerna att ha hanterats väl. Varje utförd intervju innebar ökad kunskap och större självsäkerhet och följande intervjuer kunde därmed utföras bättre. Samtliga intervjuer utfördes även verbalt, vilket gav upphov till en större möjlighet att ställa följdfrågor och få ut mer information - i jämförelse med om intervjuerna utförs över e-post. Detta anses vara en mycket positiv aspekt som även varit behjälpligt i koppling till att något färre intervjuer än förväntat utfördes. Genom att intervjuerna resulterade i en stor mängd informationsrik data, upplevdes inte avsaknaden av de ytterligare 1-2 intervjuerna som en större brist. Till följd av valet att använda intervjuer som datainsamlingsmetod, blev studien lärorik och något som författaren kommer dra stor nytta av i framtiden.

Metodvalet i form av att arbeta med en induktiv ansats och kvalitativ metod anses lämpligt eftersom det möjliggjorde för att en bredare informationsmängd kunde samlas in. Intervjuerna hölls öppna vilket bidrog till att intervjupersonerna kunde ge en större mängd information på ett mer naturligt sätt, än om det varit slutna och detaljerat strukturerade frågor. Öppna frågor möjliggjorde även för intervjupersonerna att mer spontant kunna berätta om sin verklighet i relation till det fenomen som studerats. Till följd därav kunde fler följdfrågor ställas utifrån det intervjupersonerna valde att berätta.

Ett alternativt metodval för studien hade kunnat vara att använda enkätundersökning som datainsamlingsmetod. En större mängd svar på en enkätundersökning hade eventuellt kunnat bidra till att ge en bild över hur olika utmaningar är fördelade inom olika typer av organisationer. Detta i och med att enkätundersökning är en passande metod att använda för att samla in data från en större mängd personer. Anledningen till varför detta metodval valdes bort berodde på att det beräknades bli svårt att samla in en

tillräcklig mängd svar för att kunna dra en slutsats. Ett antagande gjordes att en enkätundersökning inte skulle nå en tillräcklig mängd organisationer. Antagandet baserades på att författaren inte ansåg det troligt att intresse eller tid att besvara enkäten skulle finnas hos organisationer i en tillräckligt stor utsträckning.

8.2 Användbarhet av slutsats

Studien gjorde en avgränsning och har inte berört dataskyddsfördordningen GDPR i dess fulla helhet. Detta eftersom det hade blivit allt för omfattande och ett för brett område att undersöka. Fokus har legat på ett urval av de krav som förordningen ställer. Användbarheten av det resultat som ligger i grund till checklistan medför att slutsats och checklista ej är tillämpningsbart på alla typer av informationssystem. Hänsyn bör tas till att checklistan baserats på de resultat som gjorts i denna studie, men inte nödvändigtvis stämmer överens med alla företag och alla informationssystem. Olika krav påverkar olika företag och informationssystem på olika sätt, utifrån att de alla inte erhåller samma syfte.

Checklistan kan vara till hjälp för både utvecklare, kravställare, säkerhetsansvariga såsom VD och CIO inom olika organisationer. Även om olika kravs påverkan kan skilja sig mellan företag, kan checklistan bidra till öka en medvetenhet kring hur det bör arbetas med integritet och vilka saker som fokus bör ligga på. Checklistan kan ses som ett redskap för att säkerställa att organisationer kontinuerligt tar hänsyn till integritetsfrågor och säkerhetsåtgärder. Det kan även ses som ett verktyg för att arbetssysslor hålls konsekventa och kan hjälpa att påminna om hur arbetet bör gå till för att fortsätta vara i linje med GDPR. Checklistan bidrar även med rekommendationer för hur metoden Privacy by Design kan tillämpas och bättre uppfyllas inom system och organisation.

8.3 Vetenskapliga aspekter

I det stora hela anses resultaten av studien rimliga. Att kravet för ’Rätten att bli glömd” blev uppmärksammat av flera respondenter fanns det en föraning om redan innan studien hade påbörjats. Många befintliga informationssystem idag är exempelvis kopplade till relationsdatabaser. Detta kan innebära att de inte är byggda för den typ av raderingsfunktionalitet som GDPR kräver. ’Rätten att bli glömd’ visade sig även skapa utmaningar i koppling till loggning och backuphantering, då personuppgifter kan sparas även här. Det verkar inte ovanligt att funktionalitet för att radera enstaka eller specifika rader är något som saknas inom tjänster för loggning och backup. Det anses av författaren själv att det kan finnas en koppling till att detta krav ses som en större utmaning på grund av dessa faktorer.

Det är troligt att mycket av organisationers arbete med GDPR bör fokusera på att planera och genomföra nya och uppdaterade policys. Dessa policys bör involvera tydliga riktlinjer för vilken data som får lov att samlas in och bearbetas. Det blir även av stor vikt att säkerhetsåtgärder specificeras och att dessa ämnar minimera data och

pseudonymisera data utefter behov. De åtgärder som tas fram behöver då beröra det organisatoriska lika mycket som det berör det tekniska. Det kommer även vara nödvändigt för företag att skicka in en anmälan om en personuppgiftsincident inträffar. Det går troligen att komma längre i uppfyllandet av detta om de anställdas roller och ansvarsområden har setts över för att säkra detta krav.

En stor del av kraven ser även ut att ge upphov till en del manuellt arbete. För att långsiktigt undvika att det manuella arbetet blir för omfattande bör det budgeteras för nya informationssystem som stödjer de befintliga. Dessa nya informationssystem bör därför innehålla funktionalitet för att exempelvis hantera förfrågningar som kommer in från kunder och individer. Ett exempel skulle kunna vara frågan om samtycke och att detta registreras i det stödjande informationssystemet. Eventuellt skulle ett stödjande informationssystem också kunna hantera funktionalitet för att genomföra radering efter att en sådan förfrågan kommit in.

8.4 Samhälleliga aspekter

En effekt av GDPR ser ut att ha varit att skapa panik hos många organisationer. Särskilt mindre företag såsom startup och enmansföretag, men troligen även hos lokala bagerier, frisörsalonger m.m. som även de måste arbeta för att vara i linje med GDPR. Samtliga intervjurespondenter påpekade en viss oro, även om de alla uppgav en positiv inställning till GDPR. Bland annat fanns en viss bekymmersamhet för de indirekta skador som kan tänkas komma för mindre företag. Detta då det kan tänkas att GDPR främst vill ha åt de större företagen. Det står inte explicit i GDPR och EU har inte uttalat sig att det är fallet, men en lag som GDPR kan troligen anses ha skapats för att tygla de större drakarna. Facebook, Google och Amazon är tre stora företag som är inflytelserika på västvärldens vardag. Dessa företag sitter på mer information om de personer som använder deras tjänster än vad många troligtvis förstår. Detta inkluderar även stora mängder personuppgifter. Dessa personuppgifter kan användas för att profilera individer och sedan rikta reklam som ökar företagens omsättning. Det är dessa företag som GDPR kan ge riktlinjer och bestämmelser för hur arbetet bör se ut gällande individers personliga data. Det hjälper att säkra den personliga integriteten och upprätthåller de rättigheter som bör finnas, men som har fallit mellan stolarna när sociala medier vuxit snabbare än förväntat.

Under tiden som förberedelsearbetet inför GDPR varit i full fart skedde även en stor skandal med en av de stora jättarna, nämligen Facebook. Denna skandal involverade upp mot 87 miljoner, mestadels amerikanska, Facebook-användare. Dessa personers data sparades till en separat, privat databas utan samtycke. Insamlad data användes sedan av Cambridge Analytica, ett företag som profilerar de som röstar i uppkommande val.
I detta fall, valet i USA (Confessore, 2018). Trots att GDPR är en EU lag, måste den följas av samtliga företag som lagrar eller behandlar EU-medborgares personuppgifter. Skandalen med Facebook involverade mestadels den amerikanska befolkningen, men det väcker tankar för att något liknande kan ske i andra länder likaså. Förhoppningsvis

kan en lag som GDPR stoppa att liknande skandaler sker igen och att det kan skapa en standard för att värna om individers integritet, istället för att missbruka den.

I koppling till den omsättning som görs av dessa stora företag, väcks ett spörsmål om den sanktionsavgift som finns i GDPR. Skulle det visa sig att något av de största företagen i världen inte är i linje med GDPR, gäller det troligen inte en överträdelse så grov att det resulterar i den högsta sanktionsavgiften. Trots detta, kan det resultera i stora summor och det blir då en fråga om vart dessa pengar sedan tar vägen. Hittills framgår det ej av GDPR eller EU vad som händer med de summor som betalas ut i form av sanktionsavgifter. Personligen hoppas författaren själv att dessa pengar används i samme syfte som det som lagen står för – att skydda den personliga integriteten och säkra EU:s medborgare. Förhoppningar ligger i att pengarna används i forskningssyften och utveckling av skydd av individer och personuppgifter.

Gällande Privacy by Design uppmärksammades det att en majoritet av intervjurespondenterna uttryckte sig med en liknelse till ”sunt förnuft”. Mycket inom Privacy by Design ansågs nästan vara självklarheter, men till trots fanns en viss avsaknad av ett tänk och funktionalitet med syfte att skydda personuppgifter. Då Privacy by Design står för att hålla integriteten i fokus, upplevs det något motsägelsefullt att ej aktivt arbeta med skydd av personuppgifter, men ändå kalla metoden ”sunt förnuft”.

8.5 Etiska aspekter

Under arbetets gång har hänsyn tagits till Individskyddskravet som är framtaget av Vetenskapsrådet (2002). Samtliga fyra kategorier, informationskravet, nyttjandekravet, konfidentialitetskravet och samtyckeskravet, har därmed beaktats. Som forskare är det väsentligt att ansvar tas för att följa individskyddskravet, dels för de deltagande i studien, men även för forskaren själv.

Individskyddskravet bemöttes på så vis att innan varje intervju gavs intervjurespondenten information kring syftet med intervjun, att insamlad data enbart används till studiens forskningsändamål men delas med handledare och examinator vid Högskolan i Skövde, samt via det Digitala Vetenskapliga Arkivet DiVA. Intervjurespondenten fick även information kring hur lång tid som intervjun beräknades ta, rätten att avbryta intervjun och att få ta del av intervjun i efterhand. Intervjurespondenterna blev även tillfrågade om de samtyckte till att intervjun spelades in. Stor vikt lades också vid att hålla intervjupersonerna och de organisationer de arbetar på anonyma på en extern nivå. Inga namn på varken respondent eller organisation samlades in för att tas med i studien. Däremot hölls ej intern anonymitet under intervjuerna. Flera inom den organisation som jag samarbetat med är medvetna om vilka som ställt upp på intervju. Därmed kan det eventuellt finnas en risk att koppling mellan citat och roll i de olika organisationerna kan göras. Baserat på att respondenterna från organisationen studien utförts på känner varandra och arbetar tillsammans, samt att medvetenhet för hur det ser ut i system och organisation är

gemensam, bedömde författaren själv att denna risk sannolikt inte kommer leda till ett negativt utslag.

Vidare ingick det även författarens ansvar att med förnuft hantera det insamlade materialet på ett sådant sätt att enbart författaren själv har tillgång. Som tidigare nämnt, gjordes detta via mobil, Google Drive, anteckningsbok i enbart författarens ägor, lösenord och autentisering till författarens konto på Google Drive, lösenord och autentisering till mobil, samt lösenord till författarens privata dator.

Resultatet i form av studiens checklista är ett verktyg för olika verksamheter och företag att tillämpa, vilket även medför etiska aspekter. Det anses vara av stor vikt att det finns tillförlitlighet för det resultat som presenterats hos de som avser använda checklistan. Detta uppnås genom att checklistan är genomarbetad utifrån en noggrann datainsamling och analys. Vidare har även hänsyn tagits till att checklistan ska vara förståelig och tillräcklig för de krav och principer som berörs. Detta uppfylls genom att det gjordes en genomgående avstämning mot förordningstexten och Dr. Ann Cavoukians definitioner av de sju grundläggande principerna. Hänsyn har även tagits till att checklistan kan tillämpas av olika typer av verksamheter och företag med olika mycket resurser, vilket gör att förmåga att agera på checklistan kan se olika ut. Detta bemöts genom att svarsalternativen ges i tre mognadsgrader, samt ges flertal rekommendationer för de sju grundläggande principerna. Detta medför att checklistan är användbar för olika verksamheter med olika stor förmåga att agera på de krav som GDPR ställer.

Studiens resultat kan även bidra till upprätthållande av ett etiskt arbetssätt vid tillämpning av studiens checklista. Då GDPR har för syfte att skydda den personliga integriteten, kan detta bidra till ett ökat säkerhetstänk kring inte bara integritet, men även konfidentialitet. I huvudsak handlar GDPR om att hålla personlig data säker, men det inkluderar även ett etiskt förhållningssätt till hur personlig data används. GDPR innebär att samtliga företag som behandlar personuppgifter måste följa en striktare etisk kod för datainsamling, datalagring och datahantering. Genom studiens resultat ges verksamheter ett verktyg att tillämpa både tekniskt och organisatoriskt för att bättre vara i linje med förordningen och Privacy by Design. Därav bidrar resultatet till en positiv inverkan på den striktare etiska kod som uppförs genom att företag kan bli mer i linje med förordningen via studiens checklista.

9 Framtida forskning

GDPR är en omfattande förordning som innebär mer än det som tagits upp i denna studie. För att få en djupare förståelse för hur olika typer av företag anpassar sin organisation och sitt arbetssätt efter GDPR kan det vara betydelsefullt att undersöka både små och stora företag mer grundligt. Detta kan bidra till att ge en bild av hur förberedelsearbetet har adresserats och hur det fortlöper efter att GDPR har trätt i kraft. Framtida forskning skulle därmed eventuellt kunna ta fram vilka organisatoriska metoder som tagits fram runt om på olika företag för att bemöta hantering av persondata. Detta skulle kunna utföras med exempelvis en mer genomgående intervjustudie. Alternativt skulle även en enkätundersökning kunna bidra till att skildra hur olika företag bemöter vidareutveckling av sitt GDPR-arbete.

Vidare skulle det även vara av intresse att komplettera denna studie med att undersöka om företag bättre uppfyller de sju grundläggande principerna i Privacy by Design efter att åtgärder och förberedelser inför GDPR har implementerats i organisation och system.

Framtida forskning skulle även kunna göras i form en studie som fokuserar på vilken teknisk funktionalitet som anses mest väsentlig att implementera i nya informationssystem. I relation till GDPR:s krav, kan intresse finnas i att studera hur nyutveckling har blivit påverkad av förordningen. En fördjupningsstudie skulle kunna beröra om GDPR kan medföra att nya standarder sätts för hur företag och informationssystem ska bemöta personlig integritet.

Referenser

Ahrne, G. & Svensson, P., 2011. *Handbok i Kvalitativa Metoder*. Malmö: Liber AB.

Bell, J., 2006. *Introduktion till Forskningsmetodik.* 4 red. u.o.:Studentlitteratur AB.

Bell, J., 2010. *Doing Your Research Project.* 5 red. Glasgow: Bell and Bain Ltd..

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B., 2008. *Thesis Projects: A guide for Students in Computer Science and Information Systems.* 2:a red. London: Springer.

Bocij, P., Greasley, A. & Hickie, S., 2015. *Business Information Systems.* 5:e red. Slovakien: Pearson Education Limited.

Campbell, T., 2016. *Practical Information Security Management: A Complete Guide to Planning and Implementation.* Burns Beach: Apress.

Cavoukian, A., 2010. *Identity in the Information Society: Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D.* [Online]
Available at: https://link.springer.com/article/10.1007/s12394-010-0062-y
[Använd 12 02 2018].

Chiavetta, R., 2017. *iapp.* [Online]
Available at: https://iapp.org/news/a/survey-61-percent-of-companies-have-not-started-gdpr-implementation/
[Använd 23 02 2018].

Confessore, N., 2018. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*, 4 april. [Online]
Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
[Använd 11 05 2018]

Creswell, J. W. & Clark, V. L. P., 2007. *Designing and Conducting Mixed Methods Research.* USA: SAGE Publications, Inc..

Datainspektionen, 2017a. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/dataskyddsforordningens-syfte/
[Använd 31 01 2018].

Datainspektionen, 2017b. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/
[Använd 31 01 2018].

Datainspektionen, 2017c. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/
[Använd 12 02 2018].

Datainspektionen, 2017d. *Datainspektionen.* [Online]
Available at: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/hur-lange-far-personuppgifter-bevaras/
[Använd 12 02 2018].

Datainspektionen, 2017e. *Datainspektionen.* [Online]
Available at: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/strukturerat-eller-ostrukturerat/
[Använd 12 02 2018].

Datainspektionen, 2017f. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-radering/
[Använd 23 02 2018].

Datainspektionen, 2017g. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#1
[Använd 23 02 2018].

Datainspektionen, 2017h. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#33
[Använd 29 04 2018].

Datainspektionen, 2017i. *Datainspektionen.* [Online]
Available at:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#15
[Använd 29 04 2018].

Datainspektionen, 2018. Datainspektionen. [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/
[Använd 07 06 2018]

Degani, A., & Wiener, E., 1993. Cockpit Checklists: Concepts, Design, and Use. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *35(2)*, pp. 345-359.

Esaiasson, P., Gilljam, M., Oscarsson, H. & Wängnerud, L., 2012. *Metodpraktikan: Konsten att studera samhälle, individ och marknad*. 4:e red. Stockholm: Norstedts Juridik AB.

EU GDPR, u.d. *EU GDPR Portal.* [Online]
Available at: https://www.eugdpr.org/
[Använd 01 03 2018].

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) *Europeiska unionens officiella tidning*, Vol. L119 (4 maj 2016), pp. 1-88 [Online]
Available at: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=SV
[Använd 06 02 2018].

Gustafsson, L., Lanshammar, H. & Sandblad, B., 2009. *System och Modell - En introduktion till systemanalysen.* 1:a red. Malmö: Studentlitteratur.

Haynes, A., Weiser, T., Berry, W., Lipsitz, S., Breizat, A-H., Patchen Dellinger, E., Herbosa, T., Joseph, S., Kibatala, P., Lapitan, M., Merry, A., Moorthy, K., Reznick, R., Taylor, B & Gawande, A., 2009. *A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population. Nejm.org.* [Online]
Available at: http://www.nejm.org/doi/pdf/10.1056/NEJMsa0810119
[Använd 18 04 2018].

Holme, I. M. & Solvang, B. K., 1997. *Forskningsmetodik: Om kvalitativa och kvantitativa metoder.* 2 red. Lund: Studentlitteratur AB.

Jacobsen, J. K., 1993. *Intervju: Konsten att lyssna och fråga.* Lund: Studentlitteratur.

Jensen, M. K., 1995. *Kvalitativa metoder: för samhälls- och beteendevetare.* Lund: Studentlitteratur .

Karlström, J. (2017) *Ramverk inför dataskyddsförordningens införande: En studie över hur ett ramverk kan utvecklas för att mäta organisationers mognadsgrad.* Opublicerad kandidatuppsats från Högskolan i Skövde.

Keoshkerian, M., *Ryerson University*. [Online]
Available at: https://www.ryerson.ca/pbdi/About/Members/anncavoukian/
[Använd 13 03 2018].

King, T., 2017. *Solutions Review.* [Online]
Available at: https://solutionsreview.com/data-management/key-differences-between-

structured-and-unstructured-data/
[Använd 20 02 2018].

Lantz, A., 1993. *Intervjumetodik.* Lund: Studentlitteratur.

Lazar, J., Feng, J. H. and Hochheiser, H., 2017. *ScienceDirect.* [Online]
Available at: https://www-sciencedirect-com.libraryproxy.his.se/science/article/pii/B978012805390400008X
[Använd 07 02 2018].

Personuppgiftslag (1998:204), 3. §., 2018. *Skatteverket.* [Online]
Available at: https://www4.skatteverket.se/rattsligvagledning/27231.html?date=2018-01-01
[Använd 08 02 2018].

Reis, H. & Judd, C., 2000. *Handbook of Research Methods in Social and Personality Psychology*. Cambridge: Cambridge University Press.

Riksdagen, 1998. *Riksdagen.* [Online]
Available at: http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204
[Använd 31 01 2018].

Rännare, A. (2017) *Nya Dataskyddsfördordningens påverkan på en organisation: En fallstudie med fokus på privacy by design.* Opublicerad kandidatuppsats från Högskolan i Skövde.

SS-EN ISO/IEC 27002:2017. *Swedish Standards Institute, SIS.* [Online]
Available at: https://www.sis.se/produkter/terminologi-och-dokumentation/informationsvetenskap-publicering/dokument-for-administration-handel-och-industri/ssenisoiec270022017/
[Använd 05 02 2018].

SIS-TR 50:2015. *Swedish Standards Institute.* [Online]
Available at: https://www.sis.se/api/document/preview/8014024/
[Använd 31 01 2018].

Stair, R., Reynolds, G. & Chesney, T., 2008. *Business Information Systems.* London: Cengage Learning.

Starrin, B. & Svensson, P.-G., 1996. *Kvalitativa studier i teori och praktik.* Lund: Studentlitteratur.

Taylor, C., 2017. *Datamation.* [Online]
Available at: https://www.datamation.com/big-data/structured-vs-unstructured-data.html
[Använd 12 02 2018].

Tikkinen-Piri, C., Rohunen, A. & Markkula, J., 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34(1)*, pp.134-153.

TrustArc, 2017. *TrustArc.* [Online]
Available at: https://info.truste.com/Web-Resource-PrivacyGDPR-Research-Q22017_LP.html
[Använd 23 02 2018].

Vetenskapsrådet, 2002. *Vetenskapsrådet.* [Online]
Available at: http://www.codex.vr.se/texts/HSFR.pdf
[Använd 13 02 2018].

Åhlfeldt, R-M., Spagnoletti, P. & Sindre, G. (2007). *Improving the Information Security Model by using TFI. In Proceedings of the 22tn IFIP TC-11 International Information Security Conference* (SEC 2007). Sandton, South Africa, May 14–16, 2007. pp 73–84. ISBN: 13:978-0- 387-72366- 2, eISBN: 13:9780-387- 72367-9, ISSN: 1571–5736