INFÖRANDET AV ‘GENERAL DATA PROTECTION REGULATION’ OCH DESS PÅVERKAN PÅ SVENSKA FÖRETAG

Kandidatuppsats i Informatik

Peter Landström
Julia Ulvegärde Rombouts

2017KANI13

..

UNIVERSITY
OF BORÅS

Svensk titel: Införandet av General Data Protection Regulation och dess påverkan på svenska företag

Engelsk titel: The introduction of General Data Protection Regulation and its impact on Swedish companies

Utgivningsår: 2018

Författare: Peter Landström, Julia Ulvegärde Rombouts

Handledare: Carina Hallqvist

Abstract

At present an individual has very little control over the personal data collected, how it is used and who manages it. This is something the EU wants to change with the new General Data Protection Regulation (GDPR), which will come into force next year. The new regulation includes greater control for the individual regarding the data collected by companies. The Regulation forces companies to restructure their systems so that they are compliant with GDPR. Since high sanctions may affect those companies that do not comply with the rules, all those who handle personal data will have to review the processes that relate to the handling of personal data. The aim of this thesis is to investigate how well prepared Swedish medium to large sized companies are one year before the introduction of GDPR. The thesis focuses on how companies work with the changes from a technical perspective, an organizational perspective and from a legal perspective. With a theoretical foundation as a basis, interviews were conducted on three different companies that handle personal data, both as data controller and as data processor. The result of the study was used to design an evaluation model that companies can use one year after the introduction of GDPR. The evaluation will provide an overview of how well the transition has been and if there are any areas that need further work. There were some uncertainties regarding how the technical solutions would need to be designed and implemented to help the company being compliant with GDPR. The legal issues were largely handled through processing agreements between data controllers, data processors and third parties. The organizational perspective meant training of staff and questions regarding how to raise awareness about GDPR and the changes in working practices.

Keywords: General Data Protection Regulation (GDPR), Privacy by Design, IoT, Data Portability

Sammanfattning

I dagsläget har en individ väldigt lite kontroll över den persondata som samlas in och hur den används och vem som hanterar den. Detta vill EU ändra på med den nya dataskyddsförordningen General Data Protection Regulation (GDPR) som träder i kraft nästa år. De nya reglerna innefattar en större kontroll för individen över den data som har samlats av företag. Förordningen tvingar företag att strukturera om sina system så de är förenliga med GDPR. Då höga bötesbelopp kan drabba de företag som inte följer reglerna blir alla de som hanterar personuppgifter tvungna att se över sina processer över hanteringen. Uppsatsen har som syfte att undersöka hur väl förberedda svenska medelstora till stora företag är ett år innan införandet av GDPR och hur de arbetar med förändringarna ur ett tekniskt perspektiv, ett organisatoriskt perspektiv samt ur ett juridiskt perspektiv. Med ett teoretiskt fundament som grund genomfördes intervjuer på tre olika företag som hanterar personuppgifter i sina system, både som personuppgiftsansvariga och som personuppgiftsbiträden. Resultatet av studien användes för att designa en utvärderingsmodell som företag kan använda ett år efter införandet av GDPR. Utvärderingen kommer att skapa en överblick på hur väl övergången har gått och om det finns några områden som behöver ytterligare arbete. De slutsatser som drogs var att det fanns en del frågetecken gällande hur de tekniska lösningarna skulle se ut för att vara i linje med GDPR, de juridiska frågorna hanterades till stor del med hjälp av biträdesavtal mellan personuppgiftsansvariga, personuppgiftsbiträden och tredje part. Ur ett organisatoriskt perspektiv var det utbildning av personal och kunskap om GDPR och de ändringar i arbetssätt som detta medför.

Nyckelord: General Data Protection Regulation (GDPR), Privacy by design, IoT, Dataportabilitet

Innehållsförteckning

1 Inledning 1
1.1 Tidigare forskning 2
1.2 Problemdiskussion 4
1.3 Problemformulering 5
1.4 Syfte och forskningsfråga 5
1.5 Målgrupp 6
1.6 Disposition 6
2 Teoretiskt fundament 7
3 Metod 12
3.1 Vetenskapligt synsätt 12
3.2 Forskningsansats och strategi 12
3.3 Design av studie 13
4 Resultat och analys av det insamlade materialet 18
5 En utvärderingsmodell av hur väl organisationen uppnår kraven med GDPR 28
6 Diskussion och slutsatser 33
6.1 Metoddiskussion och –reflektion 38
6.2 Vidare forskning 41
Referenser 42
Bilagor 46
Bilaga 1 - intervjuguide 46

1 Inledning

Hur skulle du känna dig om du får reda på att data har samlats in om dig utan din vetskap och har använts för ett företags vinstsyfte? Tänk dig att du vill sluta använda en produkt, eller sluta på en arbetsplats, och vill att dina uppgifter plockas bort. Hur ska det gå till, och hur kan du veta att din data verkligen har tagits bort? De här frågorna har undersökts de senaste åren och är idag högaktuella.

Datasäkerhet är ett område som har blivit allt viktigare ju mer utspridd digitaliseringen har blivit över tid i samhället. Undersökningar som har utförts har visat en attitydförändring hos individer när det gäller vad för information och hur mycket som de är villiga att dela med sig av. General Data Protection Regulation (GDPR) har som ett av sina mål att stärka individers rätt till sin egen data och skydda individer genom att ge företag och andra organisationer regler att gå efter. GDPR består av 99 artiklar som innehåller de regler som tar upp hur personuppgifter får behandlas. Fler och fler företag livnär sig på att samla in och tolka data. Detta blir särskilt tydligt i och med den fjärde industriella revolutionen, även kallad Industri 4.0 (Näringsdepartementet 2016). Andra exempel på hur digitaliseringen förändrar samhället är Internet of Things (IoT) som blir större och större (Gartner 2015; Rudman & Sexton 2016) och e-handelsföretag som använder persondata för att optimera sin försäljning och rikta erbjudanden mot kunder (Akter & Wamba 2016). Med anledning av den stora ökningen av produkter och tjänster som IoT-produkter och sociala medier har mängden data som samlas in om användare ökat kraftigt (Ziegeldorf et al. 2014). Där individer tidigare delade med sig av persondata utan vidare eftertanke har en attitydförändring skett och med senare tiders integritetsintrång, bland annat hos myndigheter, har gjort att människor har blivit försiktigare och mer selektiva med delandet av data (Kieselmann et al. 2015, Rainie et al. 2013). Undersökningar av individers syn på datasäkerhet har utförts av företag som Fortinet (2014), Rainie et al. (2013) men även av Europeiska Kommissionen (2015).

Företag och individer står inför en utmaning som innebär att hålla data skyddad och säker. Som tidigare nämnt har det skett en attitydförändring bland individer som gör att folk är försiktigare i hur och vad de delar med sig, men ändå räcker inte det om de vill nyttja exempelvis IoT-produkter eller e-handelssidor. E-handelsföretag vill gärna samla in data från besökare för att använda detta till bland annat kundanalys som sedan kan användas för att skapa personliga rekommendationer till kunder. När det gäller IoT kan även data som har anonymiserats riskera att verka identifierande om den läggs samman med annan insamlad data. I de fall en individ äger flera IoT-produkter från samma tillverkare kan insamlad data från olika enheter läggas ihop vilket gör att det går att få ut information som inte längre är anonym (Ziegeldorf et al. 2014). Samma problem kan uppstå vid användandet av andra typer av tjänster där data kan anses vara anonymiserad, men sammanslagen med annan data verkar den identifierande. Detta beskrivs av Arvidsson och Bladh (2017) som kvasi-identifierare, en form av attribut som kan identifiera en person indirekt.

Inom Europeiska Unionen (EU) sker handel mellan de olika medlemsländerna och därmed också ett datautbyte (EUROPA 2017). Fram tills nyligen har den data som ett företag samlat in setts som företagets egendom som de kan använda som de vill. Flödet av data mellan olika länder kräver att det finns lagar som reglerar hur data får hanteras, det vill säga samlas in, bearbetas, lagras, delas och presenteras, för att skydda den personliga integriteten. 1995 togs Dataskyddsdirektivet 95/46/EG fram med syfte att stärka personers dataintegritet och balansera detta med den fria rörligheten av data inom EU. I Sverige implementerades

dataskyddsdirektivet 95/46/EG genom införandet av personuppgiftslagen (PUL) (Datainspektionen 2017). Mycket har förändrats i både samhälle och i näringslivet de senaste tjugo åren vilket gör att dataskyddsdirektivet 95/46/EG inte är anpassat efter hur data samlas in och används idag. Detta har föranlett arbetet med att ta fram ett nytt dataskyddsdirektiv. Det nya direktivet går under benämningen Regulation (EU) 2016/679 men även under namnet General Data Protection Regulation i EU vilket förkortas med GDPR. I den här uppsatsen föll valet på att använda termen GDPR eftersom det är den term som förekommit ofta i de texter vi läst då vi förkovrat oss i ämnet. I Sverige är även "dataskyddsdirektivet" ett vedertaget begrepp för detta. Ett annat begrepp som kan dyka upp i sammanhanget är "dataskyddsreformen", men detta syftar på själva arbetet med att byta från ett dataskyddsdirektiv till ett annat. Vi anser det vara mest korrekt att använda termen GDPR eftersom det då inte finns något tolkningsutrymme gällande vad som åsyftas.

På grund av det arbete som krävs för att fullständigt implementera GDPR har medlemsländerna i EU fått en tvåårsperiod på sig för att arbeta med implementeringen. I och med att GDPR börjar gälla den 25 maj 2018 står organisationer som samlar in persondata inför en utmaning (European Data Protection Supervisor 2017). GDPR innebär att individers dataintegritet kommer att skyddas i en högre utsträckning än vad som har skett tidigare och organisationer som inte uppfyller kraven kommer att kunna straffas med höga sanktionsavgifter. Förutom att personers dataintegritet ska skyddas innebär GDPR att insamlad data tillhör personen och inte företaget. Ett sätt som detta kommer att gynna individen är rättigheten till dataportabilitet, som innebär att en kund ska kunna kräva ut den data som ett företag har hämtat in om den specifika kunden (Datainspektionen 2017). GDPR kommer att ersätta personuppgiftslagen i Sverige och kommer att gälla i alla medlemsländer i EU samt de länder som hanterar data som har kopplingar till EU.

1.1 Tidigare forskning

Uppsatsen fokuserar på hur väl förberedda svenska företag är som påbörjat arbetet med övergången till GDPR. För att kunna utreda detta var det viktigt att ta reda på vad som framkommit genom tidigare utförd forskning. Eftersom GDPR har som ett av sina syften att skydda individens dataintegritet har det varit motiverat att undersöka hur individer ser på dataskydd - detta ger ett sammanhang och en bakgrund till området GDPR och informationssäkerhet ur den enskilde individens perspektiv. De nya kraven inom GDPR vad gäller förbättrad integritet och dataportabilitet gör att områden som hanterar tekniska lösningar, dataportabilitet och privacy by design, som handlar om inbyggd integritet, har varit prioriterade. Baserat på de artiklar som har lästs har vi identifierat tre olika perspektiv:

Det tekniska perspektivet fokuserar på de utmaningar som GDPR kommer att innebära för de system som företag använder, både internt och externt med samarbetspartners. *Det organisatoriska perspektivet* handlar om hur den egna personalen kommer att behöva anpassa sig, det kan handla om utbildning eller förändrade rutiner kring hantering med persondata. *Det juridiska perspektivet* fokuserar på de lagmässiga ändringar som kommer krävas av företag för att deras rutiner och avtal ska bli förenliga med de nya lagar som träder i kraft med GDPR.

Olika undersökningar har utförts för att ta reda på hur den allmänna opinionen ser ut gällande datasäkerhet. Resultatet från tidigare studier (Rainie et al. 2013) påvisade att telefonintervjuer med drygt 1000 informanter gav som resultat att 86 % av de tillfrågade hade försökt att

använda internet på ett sådant sätt som minimerar deras digitala fotavtryck. Där visades även att 55 % har aktivt försökt att undvika att bli upptäckta av specifika personer eller organisationer. Året efter utförde Lightspeed GMI på uppdrag av Fortinet (2014) en enkätundersökning som visade att informanter känner en oro över risker i form av dataintrång och exponering av personlig data. TNS Opinion & Social utförde 2015 en undersökning på uppdrag av Europeiska Kommissionen för att ta reda på EU-medborgares syn på frågor kopplade till dataskydd. Undersökningen fick namnet Special Eurobarometer och hade över 27 000 informanter. Av informanterna uttryckte omkring sju av tio tillfrågade att de kände oro för att deras information skulle användas i andra syften än det angivna syftet som informationen samlats in för ursprungligen. 69 % ansåg att deras uttryckliga tillstånd ska krävas i de fall då deras data ska samlas in och analyseras (Europeiska Kommissionen 2015).

Det tekniska perspektivet

I artikel 17 i GDPR beskrivs individens rätt att få personlig data raderad, men även kravet att också tredje part måste meddelas om att data ska tas bort. Detta skulle innebära att ett personuppgiftsbiträde skulle behöva övervaka all tillgång till data som sker, vilket enligt Kieselmann et al. (2015) skulle bli svårt att utföra. Kieselmann et al. (2015) har undersökt möjligheterna för en ny internettjänst som skulle låta individen meddela samtliga parter som hanterar dennes data att den ska tas bort.

Ett sätt för företag att få tag på den användarinformation som användare dessutom är villiga att dela med sig av är “data valorisation”, vilket innebär att ett värde sätts på olika typer av data. Perera et al. (2017) beskriver en möjlighet där individer kan få en ersättning i form av en summa pengar eller något annat av värde i utbyte för att de delar med sig av personlig data.

Engels (2016) har tittat på effekterna som GDPR och mer specifikt dataportabilitet kommer att ha på företags konkurrensmöjligheter. I sin artikel undersöker Engels hur relationerna mellan data, individer och plattformstjänster relaterar till varandra samt hur dessa relationer kommer att förändras. Artikeln undersöker specifikt vilka effekter på konkurrensen GDPR har beroende på vilken plattform som används. Artikeln delar upp plattformarna i tre olika baserat på vad för aktiviteter som individer utför på dem, nämligen sökmotorer, sociala medier och marknadsplatser.

Det organisatoriska perspektivet

Dickie och Yule (2017) skriver att en passiv eller reaktiv ansats till hur en organisation tacklar GDPR inte kommer att vara tillräckligt utan snarare leda till tänkbara sanktioner. De förespråkar privacy by design som ett lämpligt sätt att undvika fallgropar när den nya dataskyddsförordningen trätt i kraft. Privacy by design innebär att det ska finnas inbyggda mekanismer i IT-system som är till för att skydda den personliga integriteten. Motivet är att privacy by design kräver att det arbetas proaktivt med att hantera frågor som rör integritet och persondata. Vidare tar Dickie och Yule (2017) upp ett par aspekter som är viktiga när det gäller hantering av persondata för anställda. Vilken typ av data kommer hanteras? Varför, och hur kommer den att lagras? Vem har tillgång till den och varför? Hur länge ska data sparas och hur ska den skyddas, och slutligen, är det berättigat att göra det? I artikeln tar Dickie och Yule (2017) även upp ett praktiskt exempel på hur privacy by design kan implementeras vilket är genom Data Protection Impact Assessments (DPIA). I artikel 23 i GDPR tas det upp att ny teknologi ska utformas efter privacy by design (Dickie och Yule 2017). Schartum (2016) skriver att så som GDPRs artikel 23 ser ut i dagsläget riktar den sig endast mot personuppgiftsansvariga. Det är viktigt att personuppgiftsansvariga arbetar med privacy by

design då de har en stor betydelse för hur persondata skyddas och hanteras i samhället. Schartum (2016) hävdar dock att det fortfarande finns en hel del brister när det kommer till hur dataskyddsregler efterföljs och arbetet med privacy by design borde omfatta mer än bara de system som en personuppgiftsansvarig hanterar.

Det juridiska perspektivet
Ett annat begrepp som brukar nämnas i samband med privacy by design är privacy by default. Det handlar om att tjänster och produkter per automatik ska vara inställda på det högsta säkerhetsskyddet utan att användaren behöver utföra några ändringar när tjänsten eller produkten används första gången. I artikel 23 i GDPR är det fastställt att principerna privacy by design och privacy by default ska följas. Mayfield (2016) berättar i sin opinionsartikel om hur organisationer och företag i det närmaste blir tvingade att arbeta med privacy by design på grund av GDPR. Hon ser stora fördelar med det då både integriteten och säkerheten förbättras i och med pseudonymiseringen av data. Då data har blivit avidentifierad går den att använda till analyser och annan form av databearbetning. Enligt Mayfield (2016) kommer arbetet med privacy by design att leda till konkurrensfördelar då det går att marknadsföra sig själv som ett företag som tar integritet och säkerhet på största allvar.

1.2 Problemdiskussion

GDPR kommer att införas oavsett om företag är redo för det eller ej och det spelar heller ingen roll om företag har byggt upp marknadsmodeller som nu kommer att behöva förändras (Mayfield, 2016). På grund av de potentiellt höga sanktionerna som myndigheterna kan komma att ålägga företag som inte följer GDPR finns det all anledning att ta förändringen på allvar och se till att både avtal och tekniska lösningar finns på plats och fungerar som de ska.

Till följd av den tekniska utvecklingen och digitaliseringens framfart kommer det nya produkter som är optimerade för att fungera med hjälp av användares data. Men undersökningar visar att människor är oroliga för hur deras data samlas in och hanteras (Fortinet 2014). En del svarar att de till och med försöker att dölja sina digitala fotspår (Rainie et al. 2013).

Många företag livnär sig på individers data eller har det som en väsentlig del i deras affärsplanering. Dessa företag kommer att påverkas av GDPRs nya krav, såsom artikel 17. Även företag som inte har individers data som grund för deras affärsverksamhet utan främst hanterar egen, kunders och samarbetspartners data kommer att påverkas. Artikel 17 i GDPR ger individen rätt att få sin personliga data raderad. Artikeln beskriver också att tredje part måste meddelas om att data ska tas bort. Som Kieselmann (2015) beskriver gör detta att ett personuppgiftsbiträde skulle behöva övervaka all tillgång till data som sker. Eftersom detta kan bli en komplicerad uppgift har Kieselmann (2015) undersökt möjligheterna för en ny tjänst som skulle låta individen meddela samtliga parter som hanterar dennes data att den ska tas bort. EU har valt att ta fram GDPR som ett sätt för individer att återfå kontrollen över den data de delar med sig av till företag och uppdaterade riktlinjer för företag att följa. GDPR blir också ett sätt att hantera det flöde av data som rör sig mellan de olika medlemsstaterna i EU, samt mellan EU och länder som handlar med EU. Under rubriken Tidigare forskning har olika aktörer presenterats som har forskat på hantering av insamlad data från användarens och företagets perspektiv som rör GDPR och dataintegritet.

Med GDPR som kommer att träda i kraft 2018 kommer det för medborgare inom EU finnas ett tydligt regelverk för vad som klassas som personlig data hos en individ. Det kommer även att ställas högre krav på det sätt som både privata företag och statliga organ samlar in, analyserar och underhåller denna information. Den nya förordningen kommer i en allt högre grad att kräva ett mer transparent arbete där individen har rätt att få sin data raderad, rätt att veta på vilket sätt personliga data som samlats in används, samt rätten till att få tillgång till den insamlade data som finns.

Detta kommer att påverka de sätt som organisationer arbetar på och kommer även ställa krav på ändringar i hur deras system är uppbyggda. Detta kan leda till stora konsekvenser för företag som använder data till att ta fram marknadsmodeller (Mayfield, 2016) och fiktiva karaktärer för att beskriva målgrupper, som exempelvis personas (Collins och Egner 2017). Även forskningsvärlden kan påverkas genom att individer drar tillbaka sitt samtycke till att dela data på det sätt som är beskrivet av Nyrén et al. (2014). Också företag som främst hanterar sin egen personals data påverkas då GDPR kommer att gälla alla företag som hanterar personuppgifter.

1.3 Problemformulering

GDPR kommer att innebära anpassningar av system och processer, nya tekniska lösningar, ändrade avtal och förändringar i arbetssätt, och allt ska vara klart innan den 25 maj 2018. På grund av den komplexitet som kommer med införandet av en ny lag och hur företag ska efterleva denna lag vill författarna undersöka hur förberedelserna ser ut i ett avgränsat område. Med förberedelser åsyftas hur företag arbetar med och planerar övergången till GDPR. Det är mindre än ett år kvar innan GDPR träder i kraft och med stora sanktioner som möjlig följd om lagen inte efterföljs är det intressant att undersöka vilken syn företag har på GDPR samt hur arbetet ser ut. Det avgränsade området innefattar företag i Västra Götaland med fokus på de tre perspektiven som identifierats i Tidigare forskning.

1.4 Syfte och forskningsfråga

Uppsatsen har som syfte att undersöka hur väl förberedda svenska medelstora till stora företag är ett år innan införandet av GDPR och hur de arbetar med förändringarna ur ett tekniskt perspektiv, ett organisatoriskt perspektiv samt ur ett juridiskt perspektiv. För att undersöka perspektiven på ett avgränsat och väldefinierat sätt formuleras forskningsfrågan som följer:

Hur väl förberedda är svenska företag, som påbörjat övergången till GDPR, ett år innan dess införande?

1.5 Målgrupp

De resultat som framkommer i uppsatsen bedöms vara av möjligt intresse både för yrkesaktiva som arbetar med informationssäkerhet, organisation eller juridik på företag som hanterar persondata och för forskare inom informatik som vill undersöka området som rör sig mellan GDPR, informationssäkerhet och rutiner för datahantering. En utvärderingsmodell utformas utifrån resultatet av intervjuerna och kommer vara till användning för organisationer som vill bedöma hur komplett deras arbete med övergången är. Modellen kommer att ge indikationer om det finns vissa områden som behöver ytterligare arbete för att vara helt i linje med GDPR. Slutsatserna och rekommendationerna till vidare forskning kommer att ge en indikation till områden som författarna anser är värda att utforska närmare.

1.6 Disposition

Kapitel två – teori
Det teoretiska fundamentet beskriver hur andra författare ser på de områden som behandlas i uppsatsen. Det skapar den grund som intervjufrågorna baseras på och används sedan vidare i analys av empiri. Teorin är precis som i Tidigare forskning och Problemdiskussion uppdelad i de tre perspektiven teknik/IT, organisation, samt juridik och tar upp tekniska möjligheter och begränsningar, organisatoriska förändringar och möjliga svårigheter samt juridiska förändringar och de följder de kommer att leda till.

Kapitel tre – metod
I kapitel tre ligger fokus på den valda metoden och beskrivs vetenskapligt synsätt, det hermeneutiska, som även lett fram till forskningsansats (induktion) och –strategi (kvalitativ). Informationsbehovet tas fram. Design av studie beskrivs, vilket innefattar valda metoder för insamling och behandling av både teori och empiri. Här beskrivs även hur empirin leder fram till en utvärderingsmodell. Det återfinns även intervjuguide, urval och bortfall. Vidare beskriver kapitel tre reliabilitet och validitet av data, analysmetod och utvärderingsmetod.

Kapitel fyra – resultat och analys
Kapitel fyra består av empirin från de genomförda intervjuerna. Data från alla fyra informanter presenteras var för sig, och är uppdelade efter de tre perspektiven teknik/IT, organisation och juridik. I kapitel fyra återfinns även analysen som är baserad på inhämtad teori och empiri. Här jämförs svaren från alla informanter med den tidigare förförståelsen som författarna fått från teorin.

Kapitel fem - utvärderingsmodell
Med hjälp av resultaten från kapitel fyra har en utvärderingsmodell skapats som är tänkt att användas av företag ett år efter övergången till GDPR. Modellen ska användas för att se hur väl företaget möter kraven som GDPR ställer och kan hjälpa till att identifiera eventuella gap mellan nuläge och idealläge.

Kapitel sex - slutsatser och vidare forskning
Kapitel sex innehåller diskussion och slutsatser baserade på teori, empiri, analys och utvärderingsmodell samt förslag på områden för vidare forskning. Här återfinns även metoddiskussionen och det som uppsatsen syftar till att bidra med till forskningsområdet.

Avslutande del
Den avslutande delen av uppsatsen innehåller referenser och bilagor.

2 Teoretiskt fundament

General Data Protection Regulation (GDPR) kommer att påverka företag på flera olika plan och därför har teorikapitlet delats upp på ett logiskt sätt som grupperar artiklarna som refereras till under de tekniska, organisatoriska och juridiska perspektiven. Dock händer det att de olika områdena överlappar varandra. Inledningen av kapitlet består av undersökningar som har gjorts där allmänhetens åsikter och medvetenhet kring dataskydd diskuteras.

Allmänhetens åsikter och medvetenhet kring dataskydd
Rainie et al.(2013) utförde via Pew Research Center en undersökning som betalades av Carnegie Mellon University. Med hjälp av telefonintervjuer (som utfördes både på landlina och på mobiltelefon) intervjuades ett urval som bestod av 1002 personer som var 18 år eller äldre. Intervjuerna utfördes på engelska. Några av de främsta fynden var att 86 % av internetanvändare har försökt att använda internet på ett sätt som minimerar deras digitala fotavtryck. 55 % har aktivt försökt att undvika att bli upptäckta av specifika personer eller organisationer. Informanter beskriver att mycket av deras personliga data finns tillgänglig online, men de har en stark känsla av att vilja kontrollera vem som får tillgång till den. Informanterna svarade även på frågan om hur mycket de bryr sig om att endast de själva och de personer som de godkänner ska ha tillgång till information. Viktigast var innehållet i deras e-mail och personer som de e-mailar med, och minst viktigt var tiderna på dygnet som de var online.

Lightspeed GMI utförde på uppdrag av Fortinet (2014) en enkätundersökning i elva länder med 1650 deltagare med syfte att ta reda på konsumenters syn på IoT-produkter kopplade till det smarta hemmet. Undersökningen visade att informanter känner en oro över risker gällande intrång och exponering av personlig data. Tillit och privatliv var viktiga punkter för de svarande och det saknas förtroende för hur företag skulle hantera informanternas data.

År 2015 utförde TNS Opinion & Social på uppdrag av Europeiska Kommissionen en undersökning kallad Special Eurobarometer. Undersökningen var designad för att stödja slutförandet av dataskyddsreformen genom att studera vilken syn EU-medborgare har på frågor kopplade till dataskydd. Undersökningen var intervjubaserad och hade 27 980 informanter från de 28 medlemsländerna i EU. Ett område som utforskades var vikten av att kunna flytta personlig data mellan online service providers (OSP). Två tredjedelar (67 %) av informanterna ansåg att det var väldigt viktigt eller ganska viktigt att kunna flytta information som sparats från en gammal OSP till en ny. Av de tillfrågade ansåg 27 % att det inte var viktigt att kunna flytta information (Europeiska Kommissionen 2015).

Ett annat område som undersöktes var hanteringen av data av andra parter och de uppfattade riskerna kopplade till detta. Lite under tre fjärdedelar (69 %) av informanterna ansåg att deras uttryckliga tillstånd ska krävas i alla de fall där deras data samlas in och analyseras. Omkring sju av tio tillfrågade uttryckte oro för att deras information används för andra syften än det syfte som det samlades in för ursprungligen (Europeiska Kommissionen 2015).

Det tekniska perspektivet
De frågor som rör tekniska problem, möjligheter och lösningar kan ses både utifrån ett samhällsperspektiv och ur ett något smalare perspektiv, nämligen företagens. Nedan beskrivs det ur båda perspektiven för att skapa en förståelse för hur det ser ut i samhälle och näringsliv idag, och hur detta kan komma att påverka enskilda företag.

De produkter som säljs med möjligheten att koppla upp sig mot ett nätverk för att hämta uppdateringar över internet och kommunicera med andra enheter blir fler och fler. Den stora delen av dessa uppkopplade produkter samlar även in data om användaren. I dagsläget är mellan sex och nio miljarder produkter uppkopplade mot internet. Mobiltelefoner, datorer och surfplattor är exkluderade från de här siffrorna (Gartner 2015). Enligt en prognos utförd av Gartner kommer det år 2020 att finnas ca 20 miljarder uppkopplade produkter varav det största antalet kommer att vara på konsumentsidan. De räknade med en årlig ökning på 30 % från åren 2014 till 2020. Även i de här siffrorna har de valt att exkludera mobiltelefoner, datorer och surfplattor (Gartner 2015).

Termen Big Data nämns ofta i samband med IoT och det handlar om lagring av strukturerad eller ostrukturerad data i en sådan stor storlek att det är problematiskt att hantera den med traditionella databasmetoder. Olika tekniker kopplade till Big Data är exempelvis datalager och informationsutvinning (Chen och Yan 2016). I deras artikel beskriver Chen och Yan (2016) fyra olika faser som ingår i det sätt som Big Data hanterar data. Den första fasen är det sätt som IoT-produkter samlar in från sina användare, detta kan ske via olika verktyg som företag använder. Den andra fasen handlar om överföring av den insamlade informationen till molnet, som i grund och botten är servrar eller liknande datalager, där förvaring och andra processer sker. I den tredje fasen blir data analyserad och tekniker som exempelvis data mining sker. Det är här som ostrukturerad data får struktur och skapar underlag för exempelvis prediktiva modeller som söker efter mönster och kan göra förutsägelser för framtiden. Den fjärde fasen är lagring och underhåll av insamlad data.

Arvidson och Bladh (2017) har tagit upp ett problem som företag kan stöta på när GDPR har trätt i kraft. Det handlar om en punkt som tas upp i artikel 32 i GDPR och lyder som följande: *”(a) the pseudonymisation and encryption of personal data;*” (Schulz och Hennis-Plasschaert 2016). Att pseudonymisera data innebär enligt Arvidson och Bladh (2017) att de värden i en databas som är unika och identifierbara ersätts med pseudonymer eller artificiella platshållare för att minska möjligheterna att data kan användas för att unikt identifiera någon. Detta till skillnad från termen att anonymisera data, där data reduceras till den grad att det inte går att identifiera genom att i efterhand sammanställa data.

Det problem som Arvidson och Bladh (2017) presenterar handlar om vad de kallar för kvasi-identifierare vilket är attribut som kan identifiera en person indirekt. Ett identifierbart attribut kan exempelvis vara namn eller personnummer, medan ett kvasi-identifierbart attribut kan vara saker som ålder, yrke, kön och den kommun som personen är bosatt i. När dessa fyra attribut sammanställs går det att unikt identifiera ca 1% av den svenska befolkningen enligt Arvidson och Bladh (2017). Problemet som uppstår är att det är oklart vem som kommer stå till ansvar om det sker en attack eller ett intrång och därmed blir tvungen att betala de kostnader som kommer som en följd av sanktionerna som kommer att ingå i den nya dataskyddsförordningen. Blir det företaget som blir utsatt för ett intrång på sin e-handelssajt eller kommer det företag som hanterar deras data via en molntjänst att få stå för kostnaden?

Ett annat problem är att det svårt att för användaren att veta vilka data som unikt identifierar just dem (Arvidson och Bladh 2017).

En undersökning utförd av Collins och Egner (2017) på Accenture handlar om de olika förändringar som GDPR kommer att ha på organisationers sätt att arbeta med personuppgifter. En av sakerna som fokuseras på var hur data som lagras av företag måste vara portabel och möjlig att överföra. Det handlar om den nya rättighet en person har till att få tillgång till den personliga data som finns lagrad om personen. De problem som Collins och Egner (2017) lyfter handlar om att organisationer måste tillgodose en individs förfrågan om att överföra informationen i ett format som är maskinläsbart. Exempel på detta kan vara en CSV-fil, där CSV står för Comma Separated Value. För att det ska vara möjligt att överföra informationen till individen krävs det att det finns tekniska möjligheter att strukturera data på rätt sätt. Vidare tar de upp att säkra lösningar kommer behöva utvecklas för att kunna erbjuda individer en möjlighet att se eller på annat sätt ta del av den data som finns lagrad och hur den används. Collins och Egner (2017) tar vidare upp individens rätt att bli raderad. I dokumentet beskrivs ett potentiellt scenario som kan komma att uppstå när GDPR har trätt i kraft; ett företag sparar personlig information om sina kunder för att kunna skapa erbjudanden som är anpassade efter den enskilde kundens köp- och sökbeteende. När kunden begär att få sin personliga data raderad tas informationen bort, dock har företaget använt sig av denna data för att kunna ta fram olika personas som ligger till underlag för vilka affärsbeslut som är bäst. Collins och Egner (2017) ser ett dilemma huruvida företaget enligt GDPR är skyldigt att radera denna data också. Då bötesbeloppen som organisationer kan åläggas är höga är det i organisationernas intresse att personlig data hanteras på rätt sätt (Collins och Egner 2017).

Nyrén et al. (2014) beskriver hur GDPR kan ses som en risk som kommer att påverka epidemiologisk forskning om de som tillhandahåller data, data subjects, motsätter sig att vara med i undersökningen eller väljer att dra tillbaka sitt medgivande. En genomgång av de olika artiklarna som GDPR består av har jämförts med de behov som finns för att forskning inom sjukvård och hälsa samt registerbaserad forskning ska kunna bedrivas på ett säkert och opartiskt sätt.

Det juridiska perspektivet

Ziegeldorf et al. (2013) beskriver en svårighet att definiera vad personlig information och integritet innebär eftersom olika personer lägger olika värderingar i begreppen. De menar att innebörden av integritet inom området informationsintegritet innefattar självbestämmande om information vilket tillåter personen att bedöma risker angående den personliga integriteten, vidta lämpliga åtgärder för att skydda den och vara trygg i att åtgärderna efterlevs även utanför situationer som personen har möjlighet att kontrollera. Detta kan vara svårt att få att fungera i praktiken eftersom en användare kan ha flera olika IoT-produkter som visserligen enskilt anonymiserade data de samlar in, men som sedan hanterar detta på olika sätt. Ziegeldorf et al. (2013) har vidare identifierat sju olika hot mot användarens integritet där profiling ses som ett stort hot i de fall data om en och samma användare från flera olika IoT-produkter läggs samman och på så sätt kan identifiera användaren.

I april 2016 tog EU fram en ny dataskyddsförordning kallad General Data Protection Regulation (GDPR) som innehåller regler och förordningar som företag och statliga organ måste följa från och med 25 maj 2018. Den ersätter dataskyddsdirektivet 95/46/EG som togs fram 1995, och värt att notera är att den även ersätter nationella regler som exempelvis personuppgiftslagen i Sverige (Datainspektionen 2017).

I GDPR framkommer en del förändringar jämfört med dataskyddsdirektivet 95/46/EG gällande hantering av personlig data och hur denna information får användas av molntjänstleverantörer eller aktörer som arbetar med att analysera och bearbeta data. GDPR som tar upp de regler som kommer införas beskriver fyra aktörer som är involverade i hanterandet av personlig data. Aktörerna är data controller (personuppgiftsansvarig), data processor (personuppgiftsbiträde), data subject (registrerad individ) och third party (tredje part). Personuppgiftsansvarig är en juridisk person eller organisation som bestämmer över data och även ansvarar för den. Personuppgiftsbiträde är en juridisk person eller organisation som hanterar eller analyserar informationen åt personuppgiftsansvariga. Data subject är en levande individ som är kopplad eller relaterad till personlig data. Tredje part syftar på en juridisk person eller organisation som förutom data subject, personuppgiftsansvarig och personuppgiftsbiträde har tillstånd att använda personlig data. Förutom de fyra aktörerna kommer det i vissa fall krävas att företag tillsätter en data protection officer (DPO), vilket även kan kallas för dataskyddsombud. Det är en person som i sin roll ansvarar för att personuppgiftshanteringen inom företaget följer GDPR (Schulz & Hennis-Plasschaert 2016).

Vidare så tar GDPR upp nya definitioner för vad som ska klassas som personuppgifter (Schulz & Hennis-Plasschaert 2016). Några exempel på dessa är *en identifierad person*, vilket innebär en person som kan särskiljas från andra medlemmar i en grupp genom exempelvis namn, och *en identifierbar person* vilket innebär en person som direkt eller indirekt kan identifieras genom exempelvis information som en IP adress.

GDPR introducerar även nya rättigheter för den person som räknas som ett data subject. Dessa rättigheter är rätten att få sin personliga data raderad, rätten att begränsa i vilken utsträckning data får användas av personuppgiftsansvarig, rätten att få tillgång till en elektronisk kopia av den data som finns sparad och slutligen rätten till att inte utsättas för mätningsbaserad profilering (Schulz & Hennis-Plasschaert 2016). Som Ziegeldorf et al. (2013) skrev ses profilering som ett hot mot den personliga integriteten och genom att lägga till rätten att inte utsättas för mätningsbaserad profilering i GDPR ökas individens rättigheter.

Det organisatoriska perspektivet

I september 2016 genomförde Dell en enkätundersökning online där det främsta forskningsmålet var att förstå vilken uppfattning det fanns om GDPR bland individer som arbetar med och är ansvariga för att hantera privat data bland företag med europeiska kunder. 821 personer deltog i undersökningen och alla arbetade för företag där mer än 10 % av kunderna fanns i Europa. Undersökningen visade att mer än 80 % av informanterna kände att de endast visste få detaljer om GDPR eller inget alls. Mindre än en tredjedel av företagen ansåg att de var förberedda för de förändringar som GDPR kommer innebära i dagsläget. 68 % procent av de tillfrågade trodde att rollen som Data Protection Officer (DPO) kommer att tillsättas inom företaget och 18% lutade mer åt att den rollen kommer att outsourcas. Slutligen ansåg mer än 90% att deras nuvarande processer inte kommer att uppfylla de nya krav som GDPR inför (Dell 2016).

En onlineundersökning genomfördes år 2015 av företaget TRUSTe som arbetar med att hjälpa företag att uppdatera sin teknik så att de är i linje med gällande lagar och regler. Undersökningen fokuserade på vilken kunskap det fanns sedan tidigare om GDPR och vilka följder införandet av GDPR kommer att få för företag i EU och USA. Informanterna hade kunskap om datasäkerhet och antalet deltagande var 103 från USA och 99 från tre olika länder

i EU (England, Tyskland och Frankrike). En sammanfattning av resultatet visade liknande resultat som den undersökning Dell gjort när det kommer till kunskap om GDPR och arbete med förberedelser innan det träder i kraft. Hälften av informanterna saknade helt kunskap om GDPR. Av de informanter som var medvetna om GDPR var det två tredjedelar som hade börjat arbeta proaktivt med att anpassa sig efter de nya reglerna. En av slutsatserna som presenterades var det angelägna arbete som företag har framför sig där de behöver se till att deras processer och arbetssätt inte bara följer de nya regler som gäller, utan även ser till att individer med lätthet kan ta reda på vilken information som finns lagrad om dem och hur den används (TRUSTe 2015). Denna slutsats stämmer väl överens med det som presenteras av Collins och Egner (2017).

O'Brien (2017) menar att även om det är naturligt att anta att informationssäkerhet främst handlar om tekniska aspekter så inträffar de allra flesta dataintrång på grund av den mänskliga faktorn. Det kan handla om avsaknad av utbildning, rutiner som inte följs eller att en person klickar på en skadlig länk. För att komma till rätta med den här typen av svagheter inom ett företag menar O'Brien (2017) vidare att det vore bättre med ett holistiskt perspektiv på datasäkerhet där utbildning, fysisk säkerhet och skälig aktsamhet vad gäller hantering av tredje part och kontraktshantering alla får fokus. Vidare är det viktigt att avdelningar som IT, som traditionellt hanterat datasäkerhetsfrågor och juridik, som normalt sett hanterar integritetsfrågor kan samarbeta. Ett samarbete som sträcker sig över flera yrkesroller och dessutom inkluderar företagets ledning är viktigt för att frågorna om datasäkerhet och integritet inte ska hanteras som isolerade företeelser. Ytterligare aspekter som är viktiga är en öppen företagskultur vad gäller att rapportera problem, en riskhanteringsprocess som hjälper till att identifiera proaktiva åtgärder och granskning av alla de olika områdena inom företaget (O' Brien 2017).

3 Metod

De tre perspektiven av GDPR behövde granskas och då individperspektivet redan har utforskats i tidigare forskning, ofta genom enkätundersökningar, kunde detta inte hjälpa oss att svara på forskningsfrågan. Fokus i uppsatsen ligger på hur företag och organisationer hanterar datainsamling och hantering av data och för att undersöka detta var en kvalitativ ansats mer lämplig. Detta ledde till att intervjuer utfördes med informanter från olika företag vilka har valts ut baserat på särskilda kriterier som beskrivs mer utförligt nedan. Efter intervjuerna var genomförda och sammanställda togs en utvärderingsmodell fram som baserades på empirin och teorin. Modellen tar upp de fokusområden som både teorin och empirin resulterat i och presenterar en rad frågor som organisationer kan använda för att bedöma hur väl de möter kraven som GDPR ställer, utföra en analys av nuläget jämfört med det önskade läget och få en tydlig bild av om det finns något som behöver åtgärdas.

3.1 Vetenskapligt synsätt

Vårt vetenskapliga synsätt är inspirerat av hermeneutiken. Utifrån förförståelsen av teorin har informanternas svar tolkats vilket sedan har lett till ny förståelse för teorin. Då GDPR fortfarande är ett område under utveckling har det inte funnits mycket förförståelse och då har det varit tacksamt att bygga på kunskapsbasen på det hermeneutiska sättet. Enligt Eriksson och Wiedersheim-Paul (2011) handlar det hermeneutiska synsättet om metoder för insikt och tolkning av viktiga fenomen. Dessa fenomen är exempelvis dokument, handlingar eller uttalanden. I den här uppsatsen har tidigare forskning studerats och tolkats, och därefter har de insikter som gjorts använts som grund för ny datainsamling i form av intervjuer. Som beskrivet av Alvesson och Sköldberg (2008) finns det tre olika synsätt inom hermeneutiken; det objektiverande där det alterneras mellan del och helhet, det aletiska där cirkeln består av förförståelse och förståelse samt ett tredje synsätt som beskrivs av Ricœur (1981) vilket handlar om pendling mellan förklaring och förståelse. Alvesson och Sköldberg (2008) menar att de två hermeneutiska cirklarna, del-helhet och förförståelse-förståelse, inte konkurrerar med varandra eller är motsatta varandra utan snarare komplementära. Den empiri som varje intervju resulterade i gav en djupare förståelse som ledde till att nästa intervju kunde fokusera på det som var viktigt för forskningsfrågan.

3.2 Forskningsansats och strategi

Den valda forskningsstrategin för den här studien är kvalitativt inriktad där insamling av teori har skett via relevanta vetenskapliga artiklar och datainsamling för empiri har utförts genom intervjuer med vår valda målgrupp där frågorna grundades i den teori som undersökts. Valet av en kvalitativ metod för att svara på forskningsfrågan baserades på att det redan fanns gott om tidigare utförda kvantitativa undersökningar som behandlar samma område. Recker (2012) menar att kvalitativa metoder är väl lämpade i de fall ett fenomen ännu inte är utforskat ordentligt eller fortfarande är under utveckling. Då GDPR ännu inte är infört harmoniserar detta väl med ett kvalitativt metodval. Även om det fanns litteratur inom området med kvantitativt fokus var det svårare att hitta mer djupgående forskning med en större inblick i till vilken grad som företag är förberedda för GDPR. Recker (2012) beskriver att en kvalitativ metod är att föredra om det önskade resultatet handlar om att fånga vad

människor har sagt, gjort, tycker eller har erfarit av ett specifikt fenomen, ämne eller en händelse. För att skapa en förförståelse för ett relativt nytt område var det viktigt att gå igenom tidigare skriven litteratur inom området GDPR och datasäkerhet. Patton (2002) menar att en genomgång av relevant litteratur kan hjälpa till att ge en studie sitt fokus. Samtidigt uttrycker han att en litteraturgenomgång har den potentiella bieffekten att författaren kan bli partisk och därigenom göra författaren mindre mottaglig för den information som framkommer under fältarbetet (Patton 2002).

Efter genomförda intervjuer sammanställdes empirin som sedan ställdes mot teorin. Detta ledde till en förbättrad förståelse av området som helhet och gjorde att både teorin och frågor till vidare intervjuer kunde vidareutvecklas. En forskares arbete handlar bland annat om att koppla samman teori och verklighet. Tre begrepp som är kopplade till detta arbete är induktion, deduktion och abduktion. Recker (2012) skriver att induktion involverar att gå från en uppsättning specifika fakta till en mer generell slutsats eller att från observationer dra bredare slutsatser eller teorier. Induktion stämmer väl överens med hur arbetet med denna uppsats har bedrivits, då arbetsflödet har utgått från teorin för att sedan kunna dra slutsatser från den insamlade empirin. Deduktion beskrivs av Recker (2012) som att slutsatser dras utifrån givna antaganden och används vanligtvis för hypotesprövning. Enligt Patel och Davidson (2003) handlar abduktion om en kombination av induktion och deduktion. Enligt Alvehus (2013) är det vanligt att en eller annan form av abduktion praktiseras då det kan vara svårt att arbeta utifrån en rent induktiv eller deduktiv ansats.

3.3 Design av studie

Med grund i den valda forskningsstrategin beskrivs i detta avsnitt hur information har samlats in, på vilka grunder, och hur den sedan har behandlats. Forskningsstrategin som ligger till grund för uppsatsen är som tidigare beskrivet kvalitativ. I den här uppsatsen har teori använts för att skapa en grund. I kombination med inhämtade redan utförda kvantitativa och kvalitativa undersökningar och semi-strukturerade intervjuer som utförts under den här studiens livslängd har en nyanserad bild av forskningsområdet kunnat erhållas. För att besvara forskningsfrågan behövde data samlas in och analyseras från företag som kommer att påverkas av GDPR. Det var av betydelse att de tillfrågade företagen arbetade med att hantera personlig data från privatpersoner för att få en inblick i hur deras processer kring arbetet med personlig data kommer att påverkas. Vidare var det relevant att de informanter som intervjuades hade god insyn i den påverkan som GDPR kommer att innebära.

Vid insamling av teorin var två av urvalskriterierna som användes att artiklarna skulle vara vetenskapliga och referentgranskade. Artiklar som användes skulle helst inte vara skrivna senare än 2016, men sökningarna utfördes på artiklar skrivna mellan 2010 och 2017. Nyckelord som användes vid sökningarna var Big Data, Certification, Cloud computing, Data analysis, Data analytics, Data collection, Data integrity, Data portability, Data protection seals, Data revocation, Data security, General Data Protection Regulation, GDPR, IoT, Internet of Things, Privacy, Privacy by design, Privacy seals samt Security. Artiklarna hittades via sökverktygen Summon, Primo och ProQuest vilka är tre olika söktjänster där det går att hitta artiklar, uppsatser och avhandlingar med vetenskaplig anknytning. I vissa fall valdes artiklar och webbsidor ut som inte var vetenskapliga. I dessa fall tillhörde de myndigheter och ansågs de vara tillförlitliga. Några stora undersökningar som inte heller är vetenskapliga har använts. Undersökningar som blir beställda av företag med vinstsyfte kan

visa användbara resultat men resultaten bör tas med viss reservation och bör inte väga lika tungt som en vetenskaplig undersökning eller en undersökning som är beställd av en myndighet. Dessa artiklar och undersökningar hittades med hjälp av Google-sökningar med samma nyckelord som ovan.

För att samla in den empiri som krävdes för att utföra analysen genomfördes kvalitativa intervjuer. Trost (2007) tar upp termen kvalitativa intervjuer vilket beskrivs som en intervju som går ut på att förstå hur informanten tänker och känner samt vilka erfarenheter och föreställningar som den intervjuade har om området som det handlar om. Holme och Solvang (1997) skriver att syftet med en kvalitativ intervju är att öka informationsvärdet och skapa en mer heltäckande uppfattning om det valda området som studeras. Baserat på uppsatsens fokusområde var detta en passande datainsamlingsmetod då intervjuer skulle leda till en bättre förståelse av teorin. För att säkerställa att den insamlade informationen skulle vara så komplett som möjligt var tanken att intervjuerna skulle spelas in om inte informanten motsatte sig detta. Ytterligare en fördel med bandade inspelningar var att de som intervjuade skulle kunna fokusera helt på samtalet med informanten och att intervjuprocessen inte skulle störas av att anteckningar fördes under intervjuens gång. Dock finns det även nackdelar med att spela in intervjuer vilket tas upp av Alvehus (2013); en del informanter känner sig illa till mods av att spelas in och svaren blir därför inte lika spontana. Vid start av intervjuerna tillfrågades informanterna om det gick bra att intervjun spelades in. I det fall som informanten inte ville spelas in fördes istället anteckningar. Det insamlade materialet transkriberades och skickades till informanterna för deras godkännande. Att låta informanten gå igenom materialet efter intervjun är ett sätt att säkerställa att den information som informanten har förmedlat har uppfattats på rätt sätt. Det ger därigenom informanten en möjlighet att kommentera, lägga till eller ta bort saker som missats eller blivit fel. Dock finns det en möjlig nackdel med detta då informanter kan komma att redigera sina svar så att de är mer korrekta (Alvehus 2013). När valet stod mellan att låta informanter gå igenom transkriberingarna eller inte gjordes bedömningen att nyttan var större än de möjliga nackdelarna.

Urvalet av informanter och företag som kontaktats för den här uppsatsen är gjort genom en kombination av bekvämlighetsurval och strategiskt urval. Alvehus (2013) beskriver ett par olika urvalsstrategier och med dessa som grund kan det konstateras att varken ett slumpmässigt urval eller ett snöbollsurval, där redan intervjuade informanter används för att hitta fler lämpliga kandidater, var lämpliga strategier för den här uppsatsen. Ett slumpmässigt urval hade inte gjort det möjligt att säkerställa att informanterna skulle uppfylla urvalskriterierna. Ett snöbollsurval hade potentiellt lett till en visserligen bra men begränsad förståelse då variationen av informanter hade varit för liten och fokuserad. Författarna hade redan relevanta kontaktpersoner inom relevanta företag, men urvalet är inte enbart baserat på detta utan även på storlek och kriterier som beskrivs nedan. Enligt Recker (2012) litar kvalitativa metoder till ändamålsenliga undersökningar där informanter väljs ut för att de innehar vissa egenskaper som är av intresse.

De kriterier som skulle uppfyllas var:

- Informanten arbetar med hantering/processer av persondata på ett företag på en högre befattning. Det kan exempelvis vara en person som har rollen som personuppgiftsansvarige eller informationssäkerhetsansvarig
- Informanten är insatt i den nya dataskyddsförordningen GDPR
- Informanten arbetar med att anpassa verksamheten så att GDPR efterföljs när den träder i kraft

- Företag som är medelstora till stora, minst 100 anställda och som mest 3000 anställda vilket baseras på de definitioner som Europeiska Kommissionen (2017) fastställt
- Företaget kan vara personuppgiftsansvarig eller personuppgiftsbiträde

De grundläggande urvalskriterierna fungerade som stoppkriterier och avgjorde om tillfrågade individer kunde delta som informanter eller inte. Informanten behövde vara insatt i GDPR och behövde arbeta med hantering eller processarbete som rör persondata på ett företag. Valet att utesluta informanter som inte var insatta i GDPR baserades på att intervjuer med personer utan förkunskap om GDPR inte skulle ha lett till någon empiri som var till nytta för studien. Att intervjua personer som inte är insatta hade visserligen skapat en bredare förståelse överlag men fokus på studien var på de företag som aktivt arbetade med övergången till GDPR. Utöver dessa kriterier fanns det krav på storleken på företaget; Informanterna behövde arbeta på medelstora till stora företag för att det skulle kunna vara tal om en viss volym data som hanteras, och de skulle ha rutiner på plats kring hur data hanteras. För att öka reliabiliteten av den insamlade empirin var det önskvärt att intervjua informanter från ett par olika företag. För den här uppsatsen valde vi att ha fyra olika informanter där verksamheterna uppfyllde de ovanstående kriterierna men var av olika karaktär.

Andra avgränsningar har gjorts vad gäller typ av företag och storlek på företagen men även var de är lokaliserade. En grundförutsättning var att informanterna är insatta i och aktivt arbetar med övergången till GDPR, vilket gör att uppsatsen avgränsats från företag som inte är insatta i eller arbetar med GDPR. När det gäller typ av företag har vi valt att kontakta företag som främst hanterar sin egen data eller data för kunds räkning, och inte e-handelsföretag eller andra företag som samlar in och analyserar stora mängder data. Detta har sin grund i att det finns långt fler företag av vår valda typ än det finns företag som livnär sig på att samla in och analysera kunders data. De utvalda företagen är baserade i Västra Götaland då intervjuerna skulle utföras ansikte mot ansikte och ett större geografiskt område hade blivit svårt att täcka då resurserna inte fanns tidsmässigt. En avgränsning finns även från små företag. De kontaktade företagen var medelstora till stora med fler än 100 och färre än 3000 anställda. Valet på medelstora till stora företag grundar sig i att vi ville vara säkra på att de företag som tillfrågades skulle ha en viss struktur på plats inom företaget. Med detta menas en jurist som hanterar avtal, ett datorbaserat informationssystem och tillräckligt med personal för att kunna ha ett strukturerat sätt att hantera personuppgifter på, samt en viss volym persondata som hanteras. Vidare ska företaget hantera sin egen persondata, och har inte valt att lägga ut hanteringen av detta på ett externt företag. Enligt den Europeiska Kommissionen (2017) definieras medelstora företag baserat på antal anställda tillsammans med antingen den årliga omsättningen eller balansomslutningen. Ett medelstort företag har mer än 50 men mindre än 250 anställda och har antingen en omsättning som understiger 50 miljoner euro eller en balansomslutning som understiger 43 miljoner euro. Siffror som överstiger dessa gör att företag räknas som stora, och vi har valt att kontakta även stora företag. Detta motiveras av att de sanktioner som GDPR kan innebära för företag som inte följer lagen kan komma att bli mycket höga, och detta kan bli extremt kännbart för ett stort företag.

Av de tio tillfrågade företagen valde sex att inte delta. En av de tillfrågade, tillhörande ett stort företag, avböjde med kommentaren att de endast var i en inledande fas och knappt hunnit komma igång med arbetet med GDPR då de lagt sina resurser på ett systembyte. En annan tillfrågad avböjde då de var inne i en rekryteringsprocess för hitta en person som skulle jobba heltid med arbetet kopplat till GDPR. Den tredje tillfrågade avböjde med kommentar att den inte hade tid att delta. Andra tillfrågade tackade till att börja med ja till att delta men undvek

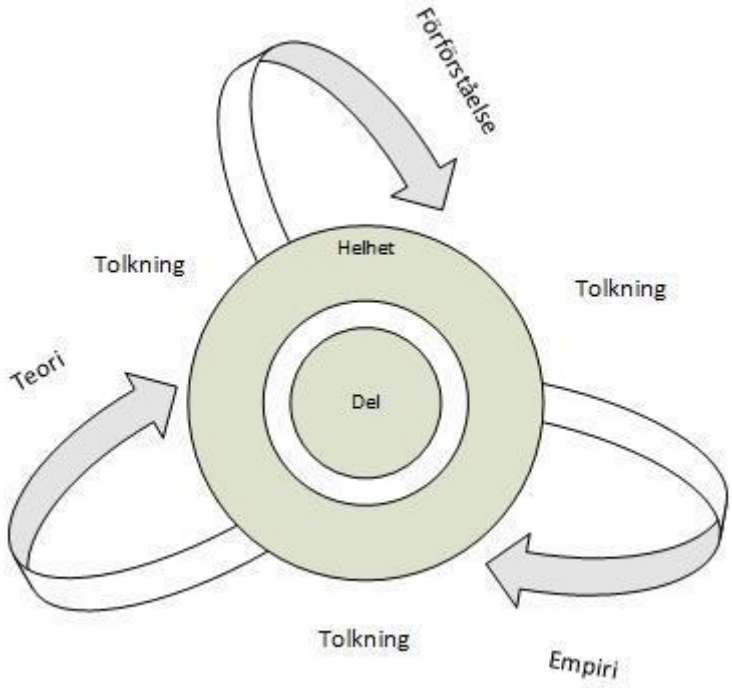
därefter att svara på vidare kontakt vilket gjorde att slutsatsen kunde dras att de inte längre var intresserade.

Det teoretiska fundamentet låg till underlag för utformningen av de frågor som användes i intervjuerna. Frågorna delades in under de olika perspektiven teknik/IT, organisation och juridik. I det tekniska perspektivet hamnade stor fokus på det arbete som informantens företag utför med att införa processer som efterföljer de rättigheter som en individ kommer att ha med GDPR. Det var framförallt dataportabilitet samt rätten att få sin data raderad som var av intresse att undersöka närmare. Detta baserades bland annat på de problem som Arvidson och Bladh (2017) lyfter med kvasi-identifierare som inte unikt kan identifiera en individ men om informationen grupperas eller sammanställs kan individer identifieras. Collins och Egner (2017) tog upp att dataportabiliteten innebär vissa svårigheter, främst att det kommer att vara problematiskt att få bort den begärda data från alla system där det sparats eller använts. För det organisatoriska perspektivet utformades frågor kopplade till utbildning av den egna personalen. Detta sågs som relevant att undersöka då det framgick i den enkätundersökning som Dell (2016) utförde att det var en majoritet av svaranden som dels ansåg att de hade för dålig kunskap om GDPR och dels ansåg att det inte fanns tillräckligt med tid för att hinna med övergången. De juridiska frågorna fokuserade på hur informanterna ska skydda sig mot sanktioner och se till att verksamheter följer alla de krav som GDPR för med sig. Det är av intresse då de nya definitioner som Schulz och Hennis-Plasschaert (2016) tar upp gällande klassificeringar av personuppgifter kommer att ställa krav på ändrade processer och rutiner för att hantera dessa personuppgifter på ett korrekt sätt. Förutom det teoretiska fundamentet användes de riktlinjer som Datainspektionen (2017) tar upp när det gäller saker som företag bör fokusera på för att vara i linje med GDPR.

Studien är utförd utifrån ett hermeneutiskt angreppssätt vilket innebär att förståelsen för forskningsområdet löpande förbättras både i del och i helhet genom tolkning (Patel & Davidson 2003). För att analysera empirin som samlats in letades efter kopplingar mellan informanternas svar och den teori som låg till grund för de områden och frågor som uppkom. Utifrån teorin analyserade vi sedan empirin för att skapa en djupare förståelse för området. Mellan intervjuerna skapades en bättre förståelse för hur arbetet med GDPR hanteras i skarpt läge, vilket medförde att nästa intervju kunde fokusera mer på de frågor som var mer relevanta. Detta var anledningen till att intervjuerna hade ett mer ostrukturerat tillvägagångssätt. Detta stöds av vad Recker (2012) beskriver; det är vanligt att insamling och analys av data antingen är sammanvävt eller till och med beroende av vartannat, till skillnad från kvantitativ forskning där de två stegen normalt sett utförs sekventiellt. Resultaten av den analyserade empirin mynnade ut i en utvärderingsmodell som presenterar frågor kopplade till de tre perspektiven samt olika kriterier som ska användas med utvärderingen. Med hjälp av utvärderingen kan organisationer skapa sig en uppfattning om hur deras arbete med omställningen till GDPR har gått och om det finns särskilda delar som kräver mer uppmärksamhet.

Enligt Esaiasson, Gilljam, Oscarsson, Towns och Wängnerud (2017) används den hermeneutiska spiralen som ett sätt att tolka eller förstå innehållet i texter. Vidare menar Esaiasson et al. (2017) att spiralen avser relationen mellan helheten och delen i ett område. För att skapa förståelse för betydelsen av en mening eller ett ord i ett specifikt textstycke måste hela texten tas i beaktning. När förståelse för vad meningen eller ordet har uppnåtts skapas en bättre förståelse för hela texten. Forskaren rör sig mellan delarna och helheten och försöker förstå om tolkningen av delen stämmer med helheten (Esaiasson et al. 2017).

Inspirerade av detta togs en egen modell fram som förklarade hur pendlingen mellan teori och empiri och den förförståelse som skapas har sett ut under arbetet med att analysera den data som samlats in genom intervjuerna. Varje iteration har ökat förståelsen för både separata delar samt hur dessa relaterar till helheten genom de tolkningar som utförts. Valet av att ta fram en egen modell istället för de som redan finns, som exempelvis den hermeneutiska cirkeln, den hermeneutiska spiralen eller Ricoeurs hermeneutiska båge som Alvesson (2008) beskriver som en variant på den hermeneutiska cirkeln, var att de inte riktigt stämde överens med det sätt som analysarbetet bedrivits under studien.



Figur 1.1 Den hermeneutiska cirkeln baserat på denna uppsats analysansats.

4 Resultat och analys av det insamlade materialet

Vi har intervjuat fyra olika representanter från tre olika verksamheter. För att kunna skilja de olika informanterna åt men ändå behålla deras anonymitet har vi valt att pseudonymisera dem. Informanterna har fått beteckningarna A, B, C och D istället för deras namn. Informationen som har hämtats in under intervjuerna har grupperats och samlats under rubriker för att förenkla läsbarheten. Detta ska inte läsas som att rubrikerna är våra intervjufrågor. Det fanns heller inget förutbestämt antal informanter utan antalet baserades dels på hur väl empirin har hjälpt till att svara på forskningsfrågan och dels på hur mycket ny data som skulle gå att få genom att utföra fler intervjuer. På grund av det iterativa arbetssätt som vi har följt har svaren vi fått lett till ökad förståelse för forskningsområdet och därmed i vissa fall lett till andra frågor i följande iterationer. Efter att all empiri var insamlad och analyserad togs en utvärderingsmodell fram som företag kan utgå ifrån för få en indikation på de områden inom perspektiven som behöver arbetas mer med för att vara i linje med GDPR.

De fyra intervjuerna genomfördes i april och maj 2017. Varje intervju skedde på plats hos informanten på dess arbetsplats med upp till en timme till vårt förfogande. Intervjuerna utfördes med enbart informanten och författarna som närvarande och där det var möjligt togs både anteckningar och spelades intervjuerna in. Informant A avböjde dock från att bli inspelad vilket gjorde att endast anteckningar togs.

Informant A arbetar som informationssäkerhetsansvarig och personuppgiftsombud på ett företag som hanterar persondata både för personal, kunder och operatörer. Informant B arbetar som bolagsjurist på ett företag som hanterar persondata för kunder och personal. Informant C arbetar som informationssäkerhetschef på ett företag där hen arbetar med informationssäkerhetsfrågor. Personuppgiftshantering ingår även som en del inom deras ledningssystem för informationssäkerhet. Informant C arbetar på samma företag som informant B. Informant D arbetar som dataskyddsombud på ett företag som hanterar persondata både för personal och kunder samt medlemmar. Företaget är ett dotterbolag till ett större företag och fokuserar på e-handel.

Intervju ett
På frågan om när arbetet med övergången till GDPR påbörjades fick vi svaret att informanten började prata om det i slutet av 2015 men fick godkänt av koncernledningen och kunde påbörja arbetet först under hösten 2016. Arbetet inleddes med en uppbyggnadsfas under ett par månader. Nu ligger fokus på inventering som sedan kommer att övergå i en aktivitetslista för vad som ska göras var och hur. Fokus kommer att ligga på tekniska lösningar och rutiner som behöver ändras. Ett exempel på detta är personal som skriver ner saker som faktiskt är personuppgifter slentrianmässigt, vilket måste ändras då det behöver finnas ett lagstöd.

Vad för typ av uppgifter samlas in och lagras?
En av de första sakerna som togs upp var vilken typ av persondata som hanterades på företaget. Informanten sa att det sparades mycket persondata från både egen personal och kunder som använder deras tjänster. Exempel på data som hanteras på personalsidan är de uppgifter som behövs för att uppfylla företagets plikter mot den anställde och gentemot olika myndigheter. Exempel på uppgifter är namn, adress, telefonnummer, anhöriga och eventuell sjukdomsbild. Exempel på uppgifter som rör kunder kan vara bilens registreringsnummer och kundens namn. Kunders uppgifter hanteras även i ett par olika tjänster som finns tillgängliga. Ett exempel på en tjänst där persondata lagrades var i form av prenumeration på nyhetsbrev

där namn och mailadress sparas. Ett annat exempel som togs upp av informanten var data från ärendehantering som exempelvis ris och ros från användare som brukat en tjänst och sedan lämnat feedback. Då lokaler hyrs ut hanteras även de personuppgifter som krävs för att avtal ska kunna gälla. För all personal, hyresgäster av lokaler och externa operatörer samlas de personuppgifter in som krävs för att riskkontroll och säkerhetsprövningar ska kunna utföras. Den intervjuade beskrev att vissa arbetsuppgifter involverar personal från andra företag och på grund av den miljö som arbetet sker i krävs det i vissa fall att riskkontroller av individer utförs. Detta innebär att persondata som exempelvis personnummer eller utdrag ur belastningsregistret kan behövas. Sen fanns det även fall där persondata från andra företag passerade genom systemen på informantens företag. I detta fall kunde det handla om information om exempelvis hyresgäster eller personal från externa operatörer.

Lagstöd, hantering och datasäkerhet

GDPR tydliggör vilket lagstöd som finns för att lagra personuppgifter. Informanten nämner att de insamlade personuppgifterna gallras med regelbundenhet. De regler som finns i PUL som gäller borttagande av uppgifter kommer att vara skärpta i och med införandet av GDPR. Organisationen som arbetsgivare är tvungen att hämta in mycket uppgifter (lagstöd, skatt, sjukpenning), men om en anställd vill bli raderad kan allt som företaget inte har lagstöd för att behålla tas bort. Ex. omdömen om den anställde. När information som personnummer och namn registreras sparas det i deras register. När data sedan inte längre behövs tas den bort enligt de föreskrifter som finns i PUL. De problem som uppstår med GDPR innefattar att det kommer att krävas en tydligare rensning enligt informanten för att inte bryta mot de förordningar som finns i GDPR. Informationen lagras i informationssystemen och det sker kontroller att data lagras och hanteras på rätt sätt. En fråga ställdes angående hur deras rutiner kring hantering av persondata ser ut när det gäller kunder som kan räknas som VIP, exempelvis en högt uppsatt politiker vilket kan innebära en högre risk. Informanten svarade att vid tillfällen där en VIP kund är inblandad så sker det en begränsad åtkomst samt även vetskap om denna information begränsas till ett färre antal personer.

Då informantens organisation är i ständig samrörelse med ett flertal andra bolag ställdes frågan om hur stort informationsutbytet är mellan bolagen och vem som ansvarar för datasäkerheten. Här tog informanten upp biträdesavtal som gör att ansvarsfrågan kan redas ut och datasäkerheten säkras. Det kan exempelvis röra sig om ett företag som erbjuder en molntjänst som hanterar persondata åt informantens företag i rollen personuppgiftsbiträde. Informanten förklarade att då det fortfarande är de som är "ägare", eller för att använda GDPRs begrepp "data controller", av den känsliga informationen krävs det att ett biträdesavtal skapas med det externa företaget. Biträdesavtalet kommer att lägga över en del av ansvaret att GDPR efterföljs och om så inte skulle ske kommer sanktioner drabba det externa företaget och inte det företag som den intervjuade jobbar för. Vidare kommer avtalet att stoppa dem från att använda data på något privat syfte, exempelvis att säljas till tredje part för marknadsföringssyfte. Informanten återkommer till området som handlar om att radera persondata, vilket är en av rättigheterna som GDPR inför för individer. Hen anser att det kommer att bli problematiskt att ta bort alla spår efter persondata som kan finnas i alla system som exempelvis loggar. Det kommet att krävas resurser och ändrade arbetsvanor med hantering av data. Vidare sa informanten att de nya regelverken kommer få konsekvenser för företag som livnär sig på att sälja personlig data. Informanten tog upp en skillnad mot dagens lagstiftning som handlade om de avtal som användare måste godkänna innan en tjänst eller produkt kan användas. I dagsläget är det tillåtet att ha regler gällande datapolicy tillsammans med resten av avtalet, men GDPR kommer införa krav att allt som har med lagring och hantering av persondata måste presenteras separat på ett tydligt sätt. Detta var något som

informanten lyfte som en klar fördel för kunden, då det inte sällan kan finnas dubbeleggade formuleringar i det finstilta i ett avtal.

Dataportabilitet

När vi kom in på området Dataportabilitet tyckte informanten att detta kommer att vara en utmaning. De tekniska lösningarna som behövs är viktiga, och rent spontant kunde det bli svårt att hinna ikapp med den här biten av GDPR innan 25 maj 2018. Informanten exemplifierade med om en organisation har 20 olika system behöver en lösning finnas som gör det möjligt att ta den data som ska exporteras ur alla system utan att en person behöver gå in och leta efter data system för system. Informanten ansåg att det kommer att kunna vara en konkurrensfördel om organisationer får ordning på dataportabiliteten eftersom det är ett komplicerat område. Det handlar om att den som begär ut sin data kommer behöva få svar snarast då GDPR kräver att det ska gå skyndsamt att lämna ut information. Dock utvecklade informanten att det är en process som kommer kräva både tid och resurser då en massa olika system behöver kommas åt för att lokalisera var kunds data finns sparad. En vidareutveckling på ämnet dataportabilitet som informanten pratade om var de möjligheter som kommer finnas för kunder att välja företag som kan importera eller exportera data. Med detta menar den intervjuade att en kund kommer vara mer benägen att välja ett företag som kan importera och exportera data på ett smidigt sätt för kunden, gentemot ett företag som inte gör det på ett effektivt och medgörligt sätt. Informanten fick en fråga som handlade om hur dataportabilitet kommer påverka deras rutiner med deras personal och som exempel togs det upp vad som kommer ske när en anställd har avslutat sin anställning och sedan begär att deras persondata ska raderas. Den intervjuade berättade att all data om den anställde som de inte har lagstöd för att behålla kommer att raderas vid en sådan begäran. Information som de kan ha lagstöd för behålls, och en regelbunden gallring sker av data som inte längre finns stöd för. Den intervjuade tar upp godkännande från en person att använda data är ett sätt när det saknas lagstöd, och att det är en sak som myndigheter och andra statliga organ ska undvika så långt det går. De måste ha lagstöd vid användandet att känslig och personlig information om individer.

Pseudonymisering, anonymisering och kryptering av uppgifter

Organisationen använder sig av applikationer och webbsidor som tjänster till deras användare där data som samlas in anonymiseras. Biometri i form av fingeravtrycksläsare var ytterligare ett ämne som kom upp, men informanten såg det inte som ett komplicerat område även om det inte är infört i dagsläget. Tanken är att användaren ger sitt tillstånd till att fingeravtrycket används under en specifik tid för att därefter raderas från systemen. Systemet med fingeravtrycksläsaren kommer dessutom vara frivilligt, och andra identifieringsmetoder kommer att finnas. Vi pratade om möjligheter till anonymisering och även kryptering. Informantens organisation tillhandahåller webbsidor och appar där data om hur dessa verktyg används och vilka sökord som är vanligast registreras och används för att optimera dessa. För att inte lagra fler personuppgifter än nödvändigt har de valt att enbart spara sökbeteenden, och inget som unikt kan identifiera en användare. När det gäller kryptering av data påpekar informanten att det kan finnas en allmän uppfattning om att det är okej att spara personuppgifter så länge som den är krypterad. Dock är krypterad persondata fortfarande persondata som de har ansvar för. Så länge som organisationen har nyckeln är de personuppgiftsansvariga. Informanten ansåg att kryptering är ett väldigt bra sätt att höja säkerheten på systemen, och trodde att alla personuppgifter i framtiden kan komma att krypteras. Ett par viktiga punkter som informanten tog upp vid ett par tillfällen var att organisationen måste ha kontroll på vad som samlas in, varför, hur det ska lagras och

hanteras. Viktigast av allt är att det ska finnas lagstöd för att uppgifter ska samlas in. När det gäller nya system som köps in måste de uppfylla kraven som ställs i GDPR. Detta enligt informanten för att inte skapa ytterligare arbete som hamnar i backloggen för att det måste anpassas efter de nya reglerna i GDPR.

Vad är den största utmaningen?
En avslutande fråga som handlade om vad informanten ansåg var den största utmaningen när det gäller att anpassa verksamheten till GDPR ställdes. Informanten ansåg att det fanns så många områden att det var svårt att välja, men valde trots detta snabbt två specifika områden som särskilt utmanande.

- Att lösa de tekniska problemen på ett skyndsamt sätt, det vill säga skapa klarhet i var uppgifterna lagras och hur kan de hanteras och raderas på ett effektivt sätt.
- Att skapa en medvetenhet hos alla medarbetare genom att utbilda och informera. Det är viktigt att personal vet hur personlig data ska hanteras. Det kommer bli viktigt att ändra på anställdas beteende och sätt att se på persondata.

Informanten avslutar med att det går fort att skriva nya regler men att få människor att anpassa sig och följa dem tar längre tid. Slutligen finns det en osäkerhet vad gäller leverantörer som kommer från länder utanför EU. Även om de ska följa GDPR för att kunna arbeta med kunder inom EU kände informanten tveksamhet för hur en leverantör från ett icke-EU-land skulle hantera en eventuell tvist och hur det skulle fungera i en domstol utanför EU. Informanten menade att organisationen såg sig om efter leverantörer som finns inom EU istället.

Intervju två
En fråga ställdes om hur länge förberedelser inför GDPR har pågått till den intervjuade. Detta var något som hen började arbeta med för ett halvår sedan men arbete med GDPR har pågått ett tag innan det. Företaget har tagit ISO/IEC certifieringen 27001 som handlar om personuppgifter, och informanten lyfte att frågan har varit viktig och central en längre tid. När förordningen antogs blev det ett intensifierat arbete för att vara redo när den träder i kraft nästa år. Informanten fick en fråga om alla förberedelser innan den träder i kraft kommer bli klara. Detta var något som var svårt att säga, målet är att bli färdiga men det finns vissa saker som kommer bli svårt att ta ställning till innan då det saknas praxis och det är osäkert exakt hur och vad som kommer krävas i detalj. Den intervjuade berättade att en ny roll på företaget kommer tillsättas som kommer att ersätta den nuvarande rollen personuppgiftsombud. Den nya rollen blir ett dataskyddsombud, det som GDPR kallar data protection officer, som kommer jobba dedikerat med frågor som rör personuppgifter och GDPR.

Vad för typ av uppgifter samlas in och lagras?
När det kommer till vilken typ av persondata/personuppgifter som hanteras på företaget sade informant B att det fanns en rad olika som strömmade igenom systemen. Det kunde röra sig om personuppgifter för anställda eller lönehantering och liknande. En annan typ var att det kunde röra sig om personuppgifter kopplade till deras kunder, exempelvis individers login eller liknande information. Vidare utvecklade informanten att de behandlar mycket personuppgifter i rollen som personuppgiftsbiträde, det som GDPR kallar data processor, det kan handla om kundens personuppgifter och deras kunder som är slutkunden. I det fallet är deras kunder personuppgiftsansvariga och sköter arbetet med att samla in personuppgifter som sedan behandlas och processas i informantens system. Den största mängden personuppgifter som behandlas på det företag informant B arbetar på är deras kunders data. Informanten säger att de varken kontrollerar syfte, ändamål eller behandling av data utan detta

sker för deras kunders räkning. Detta menar informanten innebär att de rättigheter som individer har visserligen går att rikta mot dem också, som exempelvis att hämta ut uppgifter. Hen påpekar dock att det i väldigt många fall är personuppgiftsansvarige som styr och kontrollerar även det. Vidare säger informanten att utgångspunkten någonstans är att det inte är deras uppgifter utan det är uppgifter som behandlas för annans räkning.

Hur hanteras utomstående hot eller intrång där persondata kan hamna i fel händer?
Informant B säger att vid hot eller intrång mot deras data eller mot deras kunders data finns det en skyldighet att rapportera incidenter. Detta är något som även kunderna utför. Ifall en incident skulle ske hos kund som får konsekvensen att det läcker personuppgifter hos parten som hanterar data åt dem så ser informanten framför sig att det sker en dubbel rapporteringssystem. Det finns en incident hos dem och det finns en incident hos den drabbade kunden som på ett sätt är källa till incidenten. Hur detta kommer att fungera när GDPR trätt i kraft är något som den som jobbar som säkerhetsansvarige kommer att ha koll på. Vidare säger informanten att vid en sådan incident handlar det också om att informera personuppgiftsansvarige om hur det hände. Den intervjuade sa sedan att i dagsläget så ser de över rapporteringsströmmar så de kan sätta upp hur det här ska gå till praktiskt med både skyldighet till att rapportera till personuppgiftsansvarige, som är deras kund, men även myndigheter i vissa fall där det kan finnas anmälningsskyldighet.

Privacy by design och privacy by default
En fråga ställdes om informantens företag arbetade med data protection genom privacy by design och privacy by default. Den intervjuade sa att det är något som de aktivt arbetar med, både i form av existerande system som ska ses över och även när det gäller nya system. Något som de fokuserade på var gallring av gammal data, hur det skulle gå till för att automatisera det eller på nått sätt hantera den funktionen på ett bättre sätt. En annan viktig aspekt på dessa områden som togs upp var hur informantens företag, vars centrala roll till kunden är personuppgiftsbiträde, kan säkerställa att de rutiner och system som krävs finns på plats för att uppfylla det utökade ansvaret so GDPR innebär. De fokuserar på designen, att från början bygga in systemet de instruktioner från personuppgiftsansvarige som beskriver vilken data som tas emot och hur den ska behandlas, hur länge den ska lagras och liknande instruktioner. Detta var något som den intervjuade sa var en förutsättning för att de skulle kunna vara biträde genom att uppfylla registerkraven som både personuppgiftsansvarig och personuppgiftsbiträde har att registrera all data som strömmar genom systemen. Informanten frågades ifall de som personuppgiftsbiträde måste jobba med privacy by design och privacy by default, något som GDPR uppmanar att personuppgiftsansvariga ska göra. Informant B påpekade att de i sin roll inte har ett uttryckligt krav på sig från GDPR då de behandlar data efter den personuppgiftsansvariges instruktioner. Dock fortsätter informanten med att det är något som fler och fler kommer att titta på när de väljer vilken leverantör eller samarbetspartner de vill ha. Då kravet ställs på personuppgiftsansvariga att jobba med dessa områden kommer det att leda till att de i sin tur kommer ställa krav på de verksamheter som de arbetar med, så indirekt kommer det att ställas mer krav på de som agerar som personuppgiftsbiträde.

Vad är den största utmaningen?
Informanten berättade att det fanns ett antal utmaningar. En av dessa är kartläggningen och få den på plats och en annan har med interaktion med andra att göra, att se till att det finns en samsyn på hur det ska gå till och få på plats det som saknas idag. Detta i form av avtalen som finns måste uppdateras och där det inte finns och det ska finnas och få det på plats. Även på

instruktioner och få det implementerat om det nu är så att alla bygger om sina rutiner. Deras kunder sätter nya strukturer och riktlinjer vilket leder till att nya instruktioner kommer lämnas till informantens verksamhet som de måste anpassa sig efter. Utbildning för den egna personalen är något som den intervjuade berättade kommer att ske, dock är det inte bestämt när den ska utföras. Det fanns en avvägning mellan att genomföra det nu så frågan kommer upp på bordet men fanns det arbete kvar att göra med den interna kartläggningen så det finns mer centrala och praktiska frågor att utgå från och diskutera kring.

På frågan om hur den intervjuade själv ser på GDPR så berättade hen att det fanns ett behov av en förändring av personuppgiftslagen då den var lite kraftlös. I och med de höga sanktionerna som införs med GDPR kommer den att tas på större allvar, dock känns det som att det är en ganska betungande lagstiftning för många. Ska GDPR följas korrekt så kommer det innebära mycket jobb för väldigt många bolag och att det går att funderas på proportionaliteten i det. Om de har förstått hur mycket jobb det faktiskt är, och om det kanske inte går att skydda sig även om förordningen efterföljs. Avslutningsvis ställdes en fråga om de utför mätningar eller undersökningar bland personal och hur detta kommer att påverkas. Informanten berättade att de höll på att teckna ett avtal med en samarbetspartner som kommer utföra en del sådan saker åt dem. Där ingår det ett biträdesavtal där de kommer att agera som personuppgiftsansvariga. När det kommer till personalens uppgifter fanns det lite olika sätt att gå tillväga, antingen genom samtycke eller om det finns rättslig grund för behandlingen av informationen. Det kan även vara något som krävs som en del i anställningen.

Intervju tre

Informant C fick en fråga som handlade om hur rätten att bortglömd kommer att hanteras. Den intervjuade berättade att de hanterade mycket personuppgifter åt kunders räkning som biträde, rollen som personuppgiftsansvariga var för en väldigt liten del av alla de personuppgifter de hanterar och när det gäller de egna personuppgifterna som de hanterar om de anställda så är det lite enklare hantering med manuell hantering kopplad till det. Informanten berättade vidare att för kundens räkning där det är stora volymer försöker de bygga in det i exempelvis arkiveringslösningar eller liknande lösningar så att det ska bli lätt att söka upp och sedan ta bort information om den typen av förfrågningar kommer från kunden. En följdfråga ställdes där det undrades om det var något som det aktivt arbetas med i dagsläget. Den intervjuade sa att det var det absolut, det fördes en dialog med utvecklarna så att de ska vara medvetna och mer arbete kring det kommer att ske. Vidare utvecklade hen att deras lösning har möjlighet att plocka ut en specifik personuppgift och ta bort den, så möjligheten finns inbyggd. Vidare fortsätter informanten att de ändå försöker att begränsa eller förebygga att personuppgifter kommer till dem, kunden sitter på den unika nyckeln som går att härleda till exempelvis en specifik sändning där det går att göra en koppling till personuppgifter. Hen utvecklar med att de har spartider, efter det så rensas det och det är väldigt få kunder som har arkivering med längre spartider. Beroende på hur kundens sparkrav eller lagringskrav ser ut, så säger informanten att de kan anpassa sina rutiner efter det.

GDPR och rätten till dataportabilitet

Informanten fick en fråga angående dataportabilitet och hur de arbetade med det i verksamheten. Den intervjuade ansåg att det kändes lite diffust ur deras synvinkel, och hen utvecklade att det var svårt att se hur det ska appliceras på deras verksamhet och det var ett område som de inte hade fokuserat på. Informanten fortsatte med att det finns med i deras kontrakt att som kund ska det gå att exportera sin kunddata och importera till en annan lösning och därmed ta med sig sin data. Dock så är det mer på företagsnivå och inte på

individnivå. En följdfråga ställdes som handlade om hur de skulle hantera att anställda har möjlighet att begära ut sin data. Informanten berättade att det var ett område som var ganska nytt för alla företag. Den intervjuade tänker ur deras perspektiv och berättade om deras senaste konferens där det gick ut ett allmänt utskick där olika syften och spartider togs upp och där den anställde fick samtycka eller inte samtycka kring exempelvis live-streaming och att spelas in. Detta var något som kommer att bli tydligare med bättre information för den enskilde om sina rättigheter. Informanten fortsätter med att de sparar de uppgifter som behövs så länge de behövs för att kunna upprätthålla företagets verksamhet och dess lagmässiga skyldigheter.

Medvetenhet och utbildning hos de anställda

Intervjun övergår till en fråga kring medvetenhet bland de anställda när det gäller hur personuppgifter hanteras. Informanten säger att deras företagskultur bygger på det här med att sprida information, att ha en öppen kommunikation men hen poängterar att det finns ett eget ansvar som individ också att inte sprida uppgifter i större utsträckning än vad som behövs för den tjänsten som ska utföras. De sakerna som är valfria ska det vara samtycke till, det ska även framgå i vilket syfte det lagras för och hur länge det sparas. Den intervjuade fortsätter med att det kommer att genomföras utbildning bland personalen i hur personuppgifter ska hanteras. Det hade redan utförts en awareness-utbildning för utvecklarna i ett arkiveringsprojekt där det lyfts vad som utvecklarna skulle tänka på. Vidare fortsätter hen att de även pratat om att ta fram lösningar för att underlätta både för kund och de själva gällande biträdeshanteringen. I dagsläget är den bristfällig och nu när de kommer att få ett större åtagande så säger den intervjuade att de är väldigt måna om att de har tydliga instruktioner om hur de får behandla data. Men om inte det kommer så ska de kunna skapa enkla lösningar så att det blir lätt för kunderna att lämna instruktioner och förändra instruktioner med exempelvis spartider och liknande. Informanten går igenom hur detta exempelvis kan gå till. Kunden beskriver vilka uppgifter som kommer att hanteras, att informationen inte får användas för andra syften och det kommer inte att innehålla några känsliga personuppgifter. Kunden får kryssa i det i deras gränssnitt så att de får ett godkännande. Det kan kanske vara ifyllt på förhand och det kanske inte ska gå att starta användandet av tjänsten innan den är ifylld. På så vis blir det ett moment som är obligatoriskt och därmed uppmuntras det att lämna instruktioner så att allt går till på rätt sätt utifrån kundens instruktioner.

Säkerhetsfrågor och incidenter

En fråga ställdes till informanten angående hur processen ser ut kring personuppgifts-incidenter. Den intervjuade berättade att om det är så att de hanterar personuppgifter åt en kunds räkning och det sker ett intrång där ett de får ett tapp på väldigt många personuppgifter kommer de att stå som ansvariga och dels kommer de att kunna få krav på sig från kunden och dels kommer de att få stå för eventuell skada kunden har lidit eller den yttersta personen vars uppgifter som kommit på avvägar. Sen kommer de även att kunna få viten från Datainspektionen och andra myndigheter. Informanten fortsätter med att tidigare var det bara personuppgiftsansvarige som hade det fulla ansvaret och det var väldigt låga viten generellt sett. Nu kommer det att vara både personuppgiftsansvarige samt personuppgiftsbiträdet som har ett ansvar och det är väldigt höga viten. Det var ett av skälen enligt den intervjuade att de var väldigt måna om att få tydliga instruktioner och dessutom att göra rätt. Vidare fortsätter informanten med att de ser att kunderna börjar justera avtalen nu för att sätta mer press på dem. Är det så att de har tio stora kunder och får ett skadeståndskrav som är väldigt högt så kan deras drift vara i fara för att de inte har råd att betala det vitet. Så nu ser kunder över hur mycket deras företag är försäkrat i förhållande till den mängden personuppgifter som

hanteras. Den intervjuade säger dock att de jobbar primärt med förebyggande åtgärder för att de inte ska ha några intrång.

Privacy by design och privacy by default
Informanten berättade att privacy by design och privacy by default var något som var en del i den awareness-utbildning som utvecklarna genomförde där det ska jobbas lite mer med anonymisering så att kopplingen till den faktiska personuppgiften finns hos kunden och inte hos dem. Även arbetet med med kortare gallringstider på persondata är något som arbetas med. Informanten sa även att de ville hålla på least-privileged principen, att det endast ska finnas tillgång till just precis det som behövs för att utföra sitt jobb och inte mer. Detta var något som de hade flera parallella rutiner för att säkerställa att det verkligen är så, de olika teamen på företaget som jobbar med en viss kund och har tillgång till vissa personuppgifter har bara tillgång till dem och inte till andra. Detta var både i själva applikationen men även tillgång till applikationen där personuppgifterna hanteras.

Sanktioner
En fråga ställdes till informanten om hur hen trodde att sanktionerna kommer att drabba företag som inte följer de regler som GDPR infört. Den intervjuade trodde att det kommer att ta ganska lång tid och det kommer att vara ganska många turer kring de här fallen där de kommer att pröva sig fram. Hen trodde att det till stor del kommer att bero på i vilken grad företaget har försökt att skydda sig och följa de regler och riktlinjer som GDPR har, i de fallen när ett intrång har skett och företaget har följt de regler som finns tror informanten att det kommer att vara en kraftig rabatt. Däremot i de fallen när ett företag påstår sig ha följt reglerna men inte gjort så, kommer det att bli väsentligt mycket värre. Informanten lyfter Kina som ett exempel, där det väldigt plötsligt kom en uppmaning om att de hade fram till juni på sig att anpassa sig till Kinas nya persondatalag. Hen utvecklar att det fortfarande känns som att de lever lite på de här två åren innan GDPR träder i kraft, många börjar vakna men långtifrån alla.

GDPR och konkurrensfördelar
Vi ställde en fråga om informanten ansåg att det kan vara en konkurrensfördel att förberedd när det gäller GDPR. Den intervjuade berättade att det var många av deras kunder som visat intresse för den lösningen de har gällande biträdeshanteringen som de nu ska på prov ska börja erbjuda sina kunder. Vidare säger hen att när de pratar om sina ISO-certifieringar så är det någonting som kunderna också har börjat titta på, de är även intresserade av de försäkringar som informantens verksamhet har så för dem är det en stor fördel att ha koll på både skydden och försäkringarna. Även när det kommer till upphandlingar kan det vara så att det kan spara en hel del tid, timmarna som de lägger ner på en upphandling minskar dramatiskt då allt arbete kring säkerhet och försäkringar redan finns klart för en underskrift.

Den största utmaningen med övergången till GDPR
Informanten tror att den största utmaningen blir att anpassa alla avtal. De har ett antal hundra kunder som de måste lösa det med. Att de kan känna att de kan stå för de avtalen som de har med de hanteringar som de har. När det kommer till deras egna personuppgifter tror den intervjuade att det kommer att bli jobb med det men det kommer inte vara något problem, de räknar med att de ska vara klart absolut senast till början av nästa år. De börjar med de största systemen där de lagrar internt, sen de största kunderna och ser till att de har försäkringar som täcker. Om det finns på plats tror informanten att de kommer att vara ganska nöjda om det finns på plats till maj nästa år.

Intervju fyra
Informanten berättar att hens företag började arbetet med övergången till GDPR hösten 2016. I det skedet hade inte deras moderbolag startat än utan det dröjde till januari 2017. Därefter fick informantens företag en rad olika förhållningsregler vilket ledde till att arbetet med GDPR fick göras om, detta då moderbolaget hade sina mallar och regler som det skulle anpassas till. En fråga som handlade om hur informanten personligen såg på GDPR framkom det att hen inte hade nån större koll på det fram till hösten 2016. Informanten fortsätter med att hen inte personligen har ont av att lämna ut uppgifter men att hen har fått en större medvetenhet kring vad personuppgifter kan användas till. En utmaning som informanten ser framför sig är att få marknadsdelen att förstå att de inte kan hålla på som de gör idag med att spara på all information.

Vad för typ av uppgifter samlas in och lagras?
Det är främst de uppgifter som krävs för att kunna genomföra ett avtal, som exempelvis personnummer, namn, adress och epost säger informanten tillhör de vanligaste. En följdfråga om en uppdelning på kön utförs ställs till informanten och det är något som görs på kundtjänst, även ålder används för att dela på. Informanten utvecklar att det beror på vad marknadsavdelningen vill går det att skapa profiler baserade på det. Detta är inte mer än vad kunden själv har lämnat och är inte känsliga personuppgifter.
Den intervjuade förklarar att marknadsavdelningen vill ha all information om kunden medan IT-avdelningen eller programmeraren kommer in och säger att det inte funkar att spara all information om inte data först anonymiseras eller krypteras först. Informanten tar upp ett fall som skedde nyligen där en leverantör frågade efter ålder på en specifik kund och då skickades personnumret, vilket inte var vad som efterfrågades. Informanten fortsätter med att sådana uträkningar ska ske internt och mer information än vad som efterfrågas ska inte delas ut. Detta är något som den intervjuade säger inte går att lösa med rutiner och regler utan är något som varje arbetare måste lära sig, hur det ska arbetas med eller kanske hur det frågas efter personuppgifter på ett korrekt sätt. Det svåra är att få folk att följa en rutin eller process så det blir rätt i sista ändan.

Hur kommer rätten till att bli raderad hanteras?
Informanten säger att det inte är någon som frågat om det än men att en rutin för att hantera det ska tas fram. Vidare säger den intervjuade att det inte blir en systemlösning då det förmodligen inte kommer att vara särskilt många som kommer att begära det. Det kommer istället bli en manuell rutin att plocka bort all information vid en sådan begäran, företaget har inte många olika system så det kommer inte bli så problematiskt för dom.

Vilka tekniska funktioner kommer att krävas för att följa GDPR?
Den intervjuade säger att det kommer att behövas ett register där de kan ta hand om behandlingar där det framgår när de startar och när de ska avslutas. Sen ska det finnas gallringsrutiner och vilken kategori av uppgifter som hanteras vi varje behandling. Rent generellt har deras företag kanske tvåhundra behandlingar på gång på ett eller annat sätt som rör personuppgifter och dom måste in i ett system eller en excellista. Detta ska ske i samband med ärendehanteringen, någon blir personuppgiftsägare för just den behandlingen hos företaget. Vill marknadsavdelningen få ut vilka som köper en viss vara i Borås ska det kunna göras där. Det måste dock finnas en laglig grund i att använda informationen på detta sättet, har kunden gett sitt samtycke till det. Sen säger den intervjuade att de måste locka kunden till att acceptera att deras uppgifter får användas på det viset, med exempelvis ett presentkort eller en rabatt på nästa köp. På något vis så menar hen att de köper personuppgifter till det här

ändamålet. En annan utmaning är att deras villkor ska räcka till, vilket dom inte gör idag enligt informanten. Sen måste de nå ut till en halv miljon medlemmar. Det lutar åt en ”mina sidor” eller portal för att fånga upp dom där istället. Det blir inte gratis att genomföra, vidare är det inga pengar de får igen på något sätt enligt informanten. Fördelen är att det är ett lagkrav, gör de inte det här kan straffet bli flera miljoner i böter. Informanten menar att ledningen inte kan undvika denna kostnaden, det ska göras helt enkelt och det får kosta vad det vill. Informanten säger att om de bara får ordning på deras e-handelskunder och deras medlemmar så kommer de vara i fas, kanske inte till hundra procent men de är nöjda om de kommer upp till sjuttiofem procent.

Vad blir den största utmaningen?
Informanten säger att den absolut största utmaningen blir att få alla anställda till att förstå att det inte är deras personuppgifter, utan att de måste hantera informationen på ett säkert sätt. Oavsett vad informationen används till, vilket inte sker i dag. Detta blir nog den största utmaningen. En annan utmaning blir utbildning av personal. Den interna personalen går att utbilda på en dag men det blir mer problematiskt med de 700 butiksanställda och hur de ska utbildas. Informanten säger att det arbetas på en lösning av detta och det lutar åt en distansutbildning.

5 En utvärderingsmodell av hur väl organisationen uppnår kraven med GDPR

Utifrån de tre perspektiven teknik/IT, organisation och juridik tillsammans med den empiri som har inhämtats har en utvärderingsmodell tagits fram med frågor som kan användas av företag för att se hur väl övergången till GDPR har gått. Denna utvärdering är tänkt att ske i form av en självskattning ett år efter att övergången har skett. Motiveringen till att utvärderingen bör ske efter ett år är grundar sig i att det krävs stora resurser både i form av tid, utbildning och tekniska lösningar för att möta de krav som ställs genom GDPR. Samtliga informanter lyfte, i intervjuerna, att det kommer att krävas utbildning hos personalen gällande hur data hanteras. Därmed bedömer vi det rimligt att det krävs en längre tidsperiod där nya vanor hunnit formas och har övergått i rutin innan de kan bedömas, detta gäller samtliga tre perspektiv.

Definitioner av krav och förberedelser
De deltagande behöver förstå anledningen och motivationen till utvärderingen för att ett högt deltagande ska kunna säkerställas samt att utvärderingen ska kunna hålla en hög kvalitet och generera ett pålitligt resultat (Recker 2012). Vi stödjer O'Briens (2017) åsikter om det holistiska perspektivet där olika yrkesroller samarbetar, ledningen är inkluderad i arbetet och en öppen företagskultur gör att risker kan identifieras och åtgärder kan planeras. Därför är även denna utvärderingsmodell baserad på de tre perspektiven som har identifierats och som varit och är i fokus för den här uppsatsen. Detta gör att svaren som hämtas in förväntas vara från de olika yrkeskategorierna och därigenom kunna undvika ensidiga svar.
Utvärderingars resultat påverkas av flera faktorer varav några av dessa är vem som är uppdragsgivare, vem som är utförare, vad för typ av utvärdering som utförs och varför den utförs (Zetterlund 1997). Traditionellt sett har utvärderingar setts som instrumentella och tänkta att leda till att beslut kan fattas med utvärderingen som underlag. Zetterlund (1997) menar att upplysande utvärderingar som förändrar vårt tänkande kring den utvärderade verksamheten är vanligare.

Utvärderingsmodellen som här föreslås är främst ämnad för interna utvärderingar, vilket innebär att denna utförs av en person som är anställd eller på annat sätt är verksam på det företag eller den organisation som ska utvärderas (Zetterlund 1997). Valet av den interna aktören som målgrupp för denna utvärdering är att det ger företag en möjlighet att arbeta proaktivt för att se till att de följer den nya lagstiftningen och ett sätt att identifiera områden som kan förbättras. Ett annat skäl är att de förändringar som genomförs är något som i allra högsta grad påverkar och innefattar de anställda som utför arbetsmomenten. Det kan även ses som en säkerhetsfråga då interna flöden och processer inom verksamheten inte alltid är något som en verksamhet vill exponera till en extern part.

Utformning och design av utvärderingsmodellen
Frågorna som följer är uppdelade i de tre perspektiven och består av en blandning av stängda och öppna frågor som ska kunna besvaras med ja eller nej samt med mer utförliga svar. Det finns även ett flertal ISO-standarder som kan användas, både som stöd vid en självskattning och senare för att certifiera verksamheten. Exempel på dessa är ISO 9241-11 som hanterar ergonomiska krav vid arbete som kräver en datorskärm med fokus på användbarhet (ISO.org 1998). Kriterierna är tänkta att hjälpa till att se till hur användbara de nya lösningarna, både tekniska och organisationella, är och har inspirerats av Jakob Nielsens (1999) användbarhetsprinciper. Eftersom de olika perspektiven kompletterar varandra kan vissa

frågor tänkas höra till två eller ibland samtliga tre perspektiv. Urvalet av frågor grundar sig i en kombination av teori och empiri och ska även ses utifrån dessa kriterier (ISO.org 1998):

- Användbarhet: är de nya verktygen och rutinerna lätta att lära sig och lätta att komma ihåg? Finns det dokumentation och självhjälp? Om det blir fel, är felmeddelanden då lätta att förstå? Finns det rutiner för hur organisatoriska fel ska hanteras, och är de lätta att förstå? Är de termer som används lätta att förstå?
- Effektivitet: går det att utföra arbetsuppgifter på ett enkelt och ändamålsenligt sätt?
- Tillfredsställelse: upplevs obehag vid användandet av systemen eller har användaren positiva känslor kopplade till användandet?

Frågor som rör det tekniska perspektivet

De frågor som rör det tekniska perspektivet har fokus på att det inte samlas in annan data än den som behövs för ändamålet, att data kan raderas både periodvis och på begäran av en individ samt att rätten till dataportabilitet uppfylls (Schulz & Hennis-Plasschaert, 2016). Två frågor handlar om användbarheten hos de tekniska lösningarna och om lösningarna är anpassade efter användarna. Något som lyftes av informant D var att det är viktigt att de tekniska lösningarna inte bara fungerar, utan att de även är utformade på ett sätt som gör det lätt för användarna att ta till sig det nya arbetssättet. Datainsamling är en central del i GDPR och arbetet med hur detta hanteras var något som togs upp av samtliga informanter. När det gäller rätten att bli raderad så påpekade både informant C och informant D att det till viss del skulle skötas manuellt. För informant D berodde det på att deras verksamhet inte har allt för många system och därför läggs ingen vikt på att skapa ett eget systemstöd för detta. Informant C lyfte att när det gäller rätten till att bli raderad kommer detta främst handla om den data som sparas om anställda för deras del. Dataportabilitet var en punkt som både informant A och informant C ansåg var svårtolkad. Informant A lyfte att det kommer att bli en utmaning att säkerställa att all data i alla verksamhetens system hämtas ut på ett effektivt sätt. Informant C utvecklade att de inte har påbörjat arbetet med dataportabilitet än eftersom vidare undersökning krävs för att få klart exakt hur detta ska gå till rent praktiskt. Frågor som rör yrkesroller finns med främst under den tekniska men även under den juridiska delen av utvärderingsmodellen. Då GDPR gör gällande att den personuppgiftsansvarige måste kunna visa att den nya dataskyddsförordningen följs, är detta en viktig del att lyfta i utvärderingsmodellen. Mayfield (2016) ser mycket positivt på att GDPR i princip tvingar organisationer att arbeta utifrån privacy by design; inte bara integriteten blir bättre, utan även säkerheten. Informant B var mycket tydlig med att de arbetar med privacy by design, medan informant A inte nämnde uttrycket i sig men det gick ändå att utläsa att även informant As organisation arbetar med konceptet.

Tabell 1. Det tekniska perspektivet

Nr	Fråga
1	Är de tekniska lösningarna utvecklade på ett sådant sätt att de är användarvänliga och lätta att använda?
2	Är de tekniska lösningarna anpassade utifrån de tilltänkta användarna?
Datainsamling	
3	Finns det en yrkesroll som hanterar arbetet med datainsamling?

4	Har den data som samlas in ett ändamål och används den endast till det ändamålet?
5	Är det säkerställt att de ändamål som data används till inte strider mot GDPR?
	Radering av data
6	Finns det en yrkesroll som hanterar arbetet med radering av data?
7	Finns det en teknisk lösning på plats för att radera personlig data periodvis?
8	Finns det en teknisk lösning på plats för att radera personlig data på en individs begäran?
	Dataportabilitet
9	Finns det en yrkesroll som hanterar arbetet med dataportabilitet?
10	Finns det möjlighet för en individ att begära ut sin data?
11	Kommer individen att få ut data på ett strukturerat och användbart sätt?

Frågor som rör det organisatoriska perspektivet

Undersökningar som utförts av både Dell (2016) och TRUSTe (2015) visar att den allmänna kännedomen av GDPR tidigare har varit låg. Av Dells (2016) svaranden ansåg mer än 90% att deras dåvarande processer inte skulle uppfylla de nya krav som kommer med GDPR. TRUSTe (2015) visar på liknande svar, med en relativt låg kännedom om GDPR. Vid ett flertal tillfällen har majoriteten av respondenterna talat om utmaningar som rör det organisatoriska perspektivet. Hälften av de intervjuade anser till och med att några av de största utmaningarna i övergången till GDPR kommer vara att få personalen att förstå och efterleva de nya reglerna. Dickie och Yule (2017) tar upp ett flertal aspekter som är viktiga när det gäller hantering av persondata för anställda. Genom att titta på dessa aspekter går det att skapa tydlighet i vad för data som hanteras, varför, om det är berättigat, vem som ska hantera den, samt hur länge den ska sparas och skyddas. Som tidigare nämnt menar O'Brien (2017) att det är lämpligt med ett holistiskt perspektiv på datasäkerhet. Olika avdelningar som IT och juridik behöver samarbeta och människor som hanterar personuppgifter behöver ha adekvat utbildning och rutiner som används. Informant A poängterade att det går fort att skriva nya regler men att få människor att anpassa sig och följa dem tar längre tid. Informant D pratade om svårigheter inom det organisatoriska perspektivet där det kan vara bekymmersamt att få anställda att lära sig att arbeta på rätt sätt och inte slentrianmässigt dela känslig information som är unikt identifierande. På företaget som informant C är verksam på eftersträvas det att arbeta utifrån least-privileged principen; att det endast ska finnas tillgång till just precis den information som behövs för att utföra sitt jobb och inte mer. På informantens företag råder en öppen företagskultur där kommunikation och spridning av information är viktiga komponenter. Dock har varje anställd ett eget ansvar att inte sprida uppgifter i större utsträckning än vad som behövs för det arbetsmoment som ska utföras. O'Brien (2017) pekar också på vikten av att ha en involverad och stöttande ledning för att arbetet med GDPR ska fungera bra. Informant A uttryckte att det tagit mycket lång tid från

det att hen tog upp ämnet GDPR, till att hen fick grönt ljus från organisationens ledning att påbörja arbetet.

Tabell 2. Det organisatoriska perspektivet

Nr	Fråga
1	Stöttar företagets ledning arbetet som rör GDPR och hjälper till att ge det uppmärksamhet?
2	Har anställda inom företaget utbildats för att säkerställa att de förstår GDPR och vad som krävs inom deras yrkesroll för att uppfylla de nya reglerna?
3	Har nya arbetssätt, rutiner och processer tagits fram för hantering av personlig data?
4	Finns det rutiner för kontrollera att anställda följer de nya arbetssätt som finns?
5	Finns det ett behov att informera och hjälpa anställda att ändra deras arbetssätt utöver de utbildningar som genomförts?
6	Hur hanteras den mänskliga faktorn när det gäller hanterandet av personuppgifter?
7	Har verksamheten några ISO-certifieringar som rör hantering av personlig data som exempelvis ISO/IEC 27001?
8	Hanterar anställda personuppgifter utifrån de riktlinjer som finns i GDPR?
9	Främjar kulturen inom företaget ett proaktivt arbetssätt som låter anställda belysa de brister som kan finnas gällande känslig data?

Frågor som rör det juridiska perspektivet

GDPR innebär en modernisering av tidigare personuppgiftslagar och dataskyddslagar och ger framförallt individen fler och tydligare rättigheter. Ziegeldorf et al. (2013) menar att innebörden av integritet inom området informationsintegritet innefattar självbestämmande om information. Detta tillåter personen att bedöma risker angående den personliga integriteten, vidta lämpliga åtgärder för att skydda den och vara trygg i att åtgärderna efterlevs även utanför situationer som personen har möjlighet att kontrollera. Flertalet av frågorna i det juridiska perspektivet handlar om avtal och samarbete med en utomstående part. Något som alla informanter tog upp var att när en tredje part hanterar data, eller när informanternas organisationer agerar som tredje part, så kommer ett biträdesavtal att skrivas. Ett biträdesavtal säkerställer att organisationer kan skydda sig mot de höga viten som GDPR kan dela ut till parter som inte följer lagarna. En annan fråga som tagits fram handlar om privacy by design och arbetet kring detta. Arbetet med privacy by design är en punkt som lyfts av både det tekniska och det juridiska perspektivet, vilket är något som framförallt informant C pratade mycket om. De arbetade med att anställda endast ska ha tillgång till den data som krävs för att utföra det dagliga arbetet, vilket underlättar arbetet med att vara förenlig med GDPR. Dickie och Yule (2017) skriver om hur en passiv eller reaktiv ansats till hur en organisation tacklar GDPR inte kommer att vara tillräcklig, utan snarare skapar risker att drabbas av sanktioner. Eftersom privacy by design kräver att det arbetas proaktivt med integritetsfrågor och sådant som rör persondata anses detta istället vara en lämplig ansats. En av slutsatserna som TRUSTe (2015) drog var att det arbete som företag har framför sig, där det inte enbart gäller

att ändra på processer och arbetssätt för att uppfylla de krav GDPR ställer, är att se till att individer kan ta reda på vilken information som finns lagrad och hur den används.

Tabell 3. Det juridiska perspektivet

Nr	Fråga
1	Finns det en yrkesroll som hanterar de uppgifter en personuppgiftsansvarig är ansvarig för på företaget?
2	Finns det en yrkesroll som hanterar de uppgifter ett dataskyddsombud är ansvarig för på företaget?
3	Finns det en yrkesroll som hanterar de uppgifter ett personuppgiftsbiträde är ansvarig för på företaget?
4	Finns det någon tredje part som har tillstånd att hantera personlig data?
5	Finns det avtal som reglerar hur tredje part får hantera personlig data?
6	Privatpersoner och i vissa fall anställda behöver ge sitt samtycke till att personuppgifter sparas och hanteras, finns det stöd för detta?
7	Finns det rutiner för att hantera de fall där data används för syften som inte är ändamålet?
8	Privacy by design handlar om att automatiskt använda den striktaste inställningen vad gällande integritetsskydd i produkter eller tjänster, är detta något som det arbetas med?
9	Finns det procedurer för att se till att individers rättigheter uppfylls?

Sammanfattning av utvärderingsmodellen

Vi menar att en verksamhet som har utfört en utvärdering med hjälp av vår modell ska kunna uppnå resultat som leder till nya insikter. Med detta som grund kan utvärderingen ses som upplysande (Zetterlund 1997). Resultaten ska även kunna användas som en del av ett underlag till förändringar och beslut, som ett riktmärke om de områden som behöver arbetas mer med och vilka som uppfyller kraven som GDPR infört. Zetterlund (1997) beskriver i sin bok de olika strategier som en utvärderingsmodell kan följa och den modell som denna uppsats presenterar är process-, empiri- och teoriinriktad.

I de fall en organisation inte möter alla krav för att följa den nya lagstiftningen är det viktigt att de arbetar för att nå upp till detta. De organisationer som möter kraven som lagen ställer gör klokt i att se till att de tittar på alla tre perspektiven. En balans mellan de tekniska, organisatoriska och juridiska perspektiven leder till en bättre harmoni inom organisationen då alla delarna är sammanlänkade. I båda fallen, där en organisation antingen lever upp till de krav som GDPR ställer, eller inte, går den framtagna utvärderingsmodellen att använda för att identifiera områden som kan förbättras.

6 Diskussion och slutsatser

Det tekniska perspektivet

Utifrån den insamlade teorin har vi kunnat utläsa en oro hos individer vad gäller hur deras data samlas in och hur den därefter hanteras (Fortinet 2014; Europeiska Kommissionen 2015). Medvetenheten har ökat de senaste åren vilket har gjort att folk är mer återhållsamma med sina uppgifter. Enligt undersökningen som Rainie et al. (2013) har utfört är internetanvändare till och med benägna att försöka dölja sina digitala fotspår. Sett utifrån detta är GDPR välkommet då den nya förordningen i högre grad värnar om individens rätt till sin egen data. I kontrast till detta står företagen som under många år har kunnat utveckla affärsmodeller som bygger på insamling och analyser av data som kommer att behöva ändra sina sätt att agera på (Mayfield 2016, Engels 2016). Även de organisationer som inte specifikt samlar in data för att använda den till affärsmässiga fördelar behöver tänka sig för när GDPR blir verklighet. De informanter som vi har samtalat med har sett allvaret som kommer med den nya förordningen, men även nyttan för individen. Det som Arvidson och Bladh (2017) tar upp gällande vissa icke-känsliga uppgifter som tillsammans med andra uppgifter unikt identifiera personer var något som informant D tog upp när det gällde hur, och vilken typ av data som sparas och delas.

Möjligheten att konkurrera med andra företag förändras om reglerna ändras kring hur data får hanteras. Både informant A, B och C beskrev att de såg det som en klar konkurrensfördel att som företag redan nu vara aktiva i övergången till GDPR och kunna visa upp för kunder att de följer GDPR. Detta uttryckte samtliga informanter trots att de tillhör företag som inte samlar in och analyserar data, utan huvudsakligen arbetar med data som tillhör personal, det vill säga data som krävs för att kunna bibehålla kundrelationer och data som rör samarbetspartners. Informant A och Bs tankar kring konkurrensfördelar stämmer väl överens med det som Mayfield (2016) beskriver. I intervjuerna med informant A och B framkom det att deras företag i flera fall agerade som personuppgiftsbiträden, i informant B fall var det mer fokus på denna roll än jämfört med informant A. Som Schartum (2016) skrev är det enbart personuppgiftsansvariga som är skyldiga att arbeta med privacy by design och privacy by default enligt GDPR men ändå var både respondent A och B mycket positiva till att arbeta på dessa vis.

Även om de intervjuades företag inte är tvungna att arbeta med privacy by design och privacy by default i alla situationer höll båda med om att det fanns en rad fördelar med att införa det i sina rutiner och processer genom hela systemflödet. Informant B beskrev att det även är något som hens organisation kommer att utgå ifrån när nya samarbetspartners ska väljas i de lägen när deras organisation kommer agera som personuppgiftsansvarig. Ett exempel på detta var då de i dagsläget höll på att ta fram ett avtal med en extern part som skulle hantera olika mätningar på deras persondata om de anställda. Detta pekar på att det som Schartum (2016) hävdar, nämligen att de riktlinjer som GDPR sätter upp med privacy by design bör omfatta mer än bara de system som finns hos den personuppgiftsansvarige. Det bör även omfatta de system som personuppgiftsbiträden och tredje part har. Det faktum att det inte kommer krävas av någon part utöver personuppgiftsansvariga öppnar upp för en del frågor; hur kommer mindre företag påverkas som inte har de resurser som krävs för att anpassa sina systems säkerhet? Det är inte bara systemen som behöver ändras, alla anställda kommer att behöva genomgå utbildning inom området.

Det organisatoriska perspektivet
Effekterna av GDPR ur ett företagsperspektiv kan ses på ett par olika sätt; företag som livnär sig på marknadsföring ser större svårigheter än de som enbart hanterar sina egna personuppgifter. Det finns kritiker till GDPR men även de som ser möjligheter i form av konkurrensfördelar. Att tidigt kunna visa för kunder och konkurrenter att de är aktiva i övergången till GDPR, vet vad de håller på med och så småningom kunna visa att de är fullt kompatibla med GDPR ses som positivt. Informant A nämnde att hen näst intill dagligen blev kontaktad av företag som specialiserat sig på att lotsa andra företag mot att bli kompatibla med GDPR, till skillnad från de övriga informanterna som inte sa någonting om detta. Även om den nya dataskyddsförordningen leder till mycket arbete för verksamheter, vilket samtliga informanter säger, pekar det som informant A säger om kontakten från andra företag att det även skapar arbete för en viss typ av bransch.

Informant A och B uttryckte att de var i full gång att arbeta med förberedelserna för implementationen av GDPR. Informant A uttryckte dock att det tagit mycket lång tid från att hen tog upp ämnet GDPR till att hen fick grönt ljus från organisationens ledning att påbörja arbetet. Som O'Brien (2017) nämnde är det mycket viktigt att få ledningens stöd för att kunna arbeta med GDPR på ett bra sätt och få en ökad känsla av angelägenhet inför ämnet inom företaget. Informant D pratade en del om de resurser som krävs för övergången till GDPR vad gäller kostnader för systemändringar och även den tid det kommer att ta att utbilda personalen i hur persondata ska hanteras. Informant D ansåg att det sannolikt skulle bli en del problem med utbildning av personal, inte vad gäller utbildning av personalen på huvudkontoret men däremot med de cirka 700 anställda som jobbar ute i butiker. Vidare menade hen att det inte är några större problem att ta fram en ny rutin eller process men det är svårare att få folk att hantera personuppgifter på ett korrekt sätt. En ytterligare kommentar från informant D är att då GDPR är en lag så har en företagsledning inget val än att gå med på den kostnaden som övergången innebär.

Vidare lyfte informant A och B att det kommer vara ett mödosamt arbete med att radera all data om en användare begär det. Informationen finns utspridd över flera olika system internt hos personuppgiftsansvarige men även i system hos personuppgiftsbiträdet samt de tredje parter som fått ta del av data. Det finns ett behov för den tjänst som Kieselmann et al. (2015) tittat på där användaren kan meddela alla parter som hanterar dess data att den ska raderas. Detta var något som informant D tog upp då deras företag ansåg att det inte var värt att ta fram en systemlösning för denna uppgift. Detta motiverades med att hen ansåg inte att det skulle vara så många personer som skulle begära att deras information ska raderas. Istället beskrev informant D en manuell process där en anställd skulle få ansvaret för ett ärende och sedan se till att ta bort all den information som inte ska sparas manuellt. Som O'Brien (2017) tar upp är den mänskliga faktorn den största orsaken till brister som leder till dataintrång vilket både informant C och D pratade om när det gäller att få människor att hantera känslig data på rätt sätt. Båda informanterna lyfte att utbildningar skulle genomföras men samtidigt menade båda att det inte kommer att räcka. Informant D tog upp att det är lätt att införa nya rutiner eller processer men det har ingen betydelse om en anställd inte hanterar data på ett säkert sätt. O'Brien (2017) menar att det är viktigt med en öppen företagskultur när det gäller att rapportera problem och även att identifiera proaktiva åtgärder för att vara förberedda för problem som kan uppstå.

Det juridiska perspektivet

Undersökningar har visat att människor är oroliga för hur deras data samlas in och hanteras (Fortinet 2014, Europeiska Kommissionen 2015). Då personuppgifter flödar mellan olika länder finns det ett behov av att på europeisk nivå kontrollera hur data får lov att hanteras. Detta ämnar EU uppnå med den dataskyddsförordningen som ersätter de nationella skydd som respektive EU-land har i dagsläget. Forskningen pekar på att det fortfarande finns många frågetecken på exakt hur vissa områden inom GDPR ska tolkas. Detta var något som lyftes av informant B, att det fanns oklarheter i hur vissa delar av GDPR skulle hanteras för att vara förenliga med reglerna. De intervjuade såg främst på hanteringen av data och GDPR ur ett legalt och tekniskt perspektiv, inte nödvändigtvis ur ett användarperspektiv. Samtidigt som det fanns en gemensam känsla av att GDPR innebär mycket arbete var både informant A och B positiva till den nya förordningen då de såg till fördelarna som privatpersoner och inte som representanter för organisationer.

Sett ur ett företagsperspektiv verkar de företag som arbetar som data processor inte få några stora bekymmer i framtiden när de väl är kompatibla med GDPR. Både informant A och B nämnde biträdesavtal som en viktig ingrediens i receptet för att kunna lyckas när GDPR väl är implementerat. Däremot kan företag som livnär sig på att samla in data få det svårare då användare uttryckligen måste godkänna behandlingen av deras uppgifter. Snarare blir det individen som själv kommer kunna bestämma vart deras data får användas och i vilken utsträckning. Det område som Perera et al. (2017) tog upp om att användare kan få ersättning i utbyte för att de villigt delar sin data kan leda till att nya möjligheter öppnas upp för hur persondata hanteras. Företag kommer behöva vara mer transparenta med hur de hanterar kundens data för att locka till sig kunder, detta var något som informant D lyfte under intervjun. För att marknadsavdelningen på dennes företag ska kunna använda kunders information krävs det ett incitament för att få kunden att gå med på att deras personuppgifter används. Informant D tog som exempel upp ett presentkort eller en rabatt som kan användas vid nästa köp. Alla fyra informanterna såg med förståelse på de höga sanktioner som kan komma att drabba företag som bryter mot GDPR. En kommentar var att PUL har varit tandlöst, vilket har gjort att företag har kunnat göra lite som de själva har velat.

Slutsatser

Forskningsfrågan *Hur väl förberedda är svenska företag, som påbörjat övergången till GDPR, ett år innan införandet?* har följt arbetet genom denna uppsats, och vi anser den vara besvarad. Med hjälp av resultaten som framkom genom våra intervjuer valde vi att ta fram en utvärderingsmodell som verksamheter kan använda för att skapa sig en uppfattning om hur väl de möter de krav som GDPR ställer på dem och identifiera saker som kan behöva förbättras.

I skrivande stund är det mindre än ett år kvar till att GDPR träder i kraft. Vi ser att företag arbetar med sina övergångar men att det fortfarande finns frågetecken vad gäller de tekniska lösningarna. De juridiska frågorna löses bland annat med biträdesavtal och av den information som framkom genom intervjuerna är den juridiska biten mindre komplicerad än vad de tekniska lösningarna är. En utmaning som samtliga informanter framhöll var hur GDPR skulle hanteras rent organisatoriskt i form av ändrade arbetssätt och attityder hos anställda. Något som var förvånande var att informanterna inte hade lika mycket funderingar kring de tekniska lösningarna som hade antagits vid ett tidigt skede av studien. Ytterligare ett antagande som gjordes tidigt i studien var att företag skulle vara mycket insatta och engagerade i en lagändring som skulle innebära potentiellt höga viten. Istället för att detta bekräftades nekade flera företag att delta i intervjuer, ofta med anledningen att de inte kommit tillräckligt långt i arbetet med övergången till GDPR, eller ens påbörjat arbetet. För att exemplifiera hade en organisation som kontaktades precis påbörjat arbetet med att rekrytera en person som skulle arbeta med övergången, och i en annan organisation var de upptagna med ett systembyte och hade därför inget fokus på arbetet med anpassningen till GDPR. Vi har identifierat ledningens stöd som en nyckelfaktor i ett lyckat arbete med övergången till GDPR. Både i teori och empiri framkommer hur viktigt det är. Informant A poängterade hur hen hade tagit upp ämnet GDPR vid upprepade tillfällen under en längre tid innan ledningen gav starttecken till att påbörja arbetet. Den här insikten gör att vi kan anta att ledningen i de verksamheter som tackade nej till att delta i vår studie inte prioriterade arbetet med GDPR. Det kan även innebära att samarbetet mellan olika avdelningar inte var optimalt hos dessa verksamheter.
Överlag verkar de organisationer som är medvetna om GDPR vara väl insatta i de förändringar som krävs men det finns oklarheter kring hur vissa delar ska genomföras rent praktiskt, särskilt rätten att bli raderad och rätten till att få ut sina personuppgifter. Flera av informanterna tog upp att dessa rättigheter var svåra att förbereda sig för. Tre av informanterna trodde att det kommer att bli tydligare när GDPR väl trätt i kraft och bättre förhållningsregler tagits fram. Både informant B och D var inte särskilt oroliga för höga viten det första året så länge som det inte handlade om grovt missbruk av personuppgifter. Detta känns rimligt då det vore oskäligt att förvänta sig att alla företag kommer att ha allt klart till hundra procent när GDPR träder i kraft. Samtidigt finns det ingen övergångsperiod inplanerad utan GDPR träder i kraft med full effekt 25 maj 2018 vilket skulle innebära att de som inte följer GDPR kommer att drabbas av viten omgående. Då myndigheter bör ha svårt att kontrollera hur väl företag efterlever kraven som GDPR ställer på dem ser vi det som rimligt att informant B och Ds antaganden kan stämma.

Företag som i huvudsak hanterar sin egen personals data och inte arbetar med datainsamling och analys av data, som är fallet hos e-handelsföretag, kan lösa många av sina problem med hjälp av biträdesavtal. Den juridiska aspekten är stor och kommer leda till konsekvenser för de företag som inte kan uppfylla de krav som ställs på de som hanterar persondata på beställning av en annan part. Samtidigt kommer det att leda till konkurrensfördelar för de företag som genomfört övergången i tid. En annan aspekt är de nya möjligheter som GDPR

innebär ur ett affärssammanhang, att individen får mer kontroll över sin persondata innebär att kunden kommer få mer att säga till om. Företag som sköter säkerheten bra och även erbjuder förmåner i utbyte för att få lov att bearbeta kunders data kan ha lättare att locka till sig kunder som är måna om det sätt som deras data hanteras på. Detta känns som en rimlig utveckling när individen får större kontroll över sin egen information men det är ändå en verklig möjlighet att det blir få personer som verkligen tar till vara på detta. Företag som väljer att tidigt anpassa sig till denna utveckling kan få det lättare att knyta till sig nya kunder som är medvetna om de rättigheter som de har. För dessa företag blir det viktigt att individer informeras om lagändringen och vad den kommer att innebära för dem. Företagen spelar en roll i detta, både genom att marknadsföra sig som ett företag som tar hand om individers data på rätt sätt och genom att konkurrera ut andra företag som inte har hunnit lika långt i utvecklingen. En annan viktig aktör bör vara myndigheter som har en möjlighet att informera allmänheten i stort om deras rättigheter och möjligheter. En vidare möjlighet är att myndigheter kan stödja företagen med rådgivning, riktlinjer och tips om hur tjänster kan förbättras. Om inte myndigheter kommer att fungera som stöd finns det en möjlig öppning för företag inom den privata sektorn som har specialiserat sig på GDPR att bistå med sina tjänster. Informant A lyfte i intervjun att hen nästintill dagligen fått telefonsamtal från företag som ville hjälpa till med övergången till GDPR.

GDPR är tänkt att möta nutidens krav på en lagstiftning som kan hantera utvecklingen ur ett näringslivsperspektiv och tekniskt perspektiv. Dataskyddsdirektivet 95/46/EG som infördes 1995 var i behov av en uppdatering. Det har hänt mycket sedan dess när det kommer till hur teknik och tjänster kommunicerar och samlar in data och ett nytt regelverk var behövligt. Det är dock svårt att avgöra innan det trätt i kraft just hur effektivt det är när det kommer till att stärka integriteten för individen.

Den här studien syftar till att bidra med nya insikter till forskningsområdet och gör detta genom att ge en inblick i hur övergången till GDPR ser ut i näringslivet i medelstora till stora företag. Dessa företag anses ha en högre risk av att drabbas av sanktioner än vad mindre företag skulle göra om reglerna inte följs då de har fler kunder och därmed antas hantera fler personuppgifter. Resultaten av den första delen av studien visar att även om de informanter som har intervjuats är medvetna om och arbetar med GDPR så finns det fortfarande frågetecken och en tveksamhet till om det är möjligt att följa den nya lagen fullt ut när den införs. På grund av detta ser vi en öppning för att studera både hur myndigheter kommunicerar viktig information som denna och hur företag arbetar med att lösa de problem som de stöter på. Eftersom hanteringen av personuppgifter utifrån GDPR är ett område som sträcker sig över flera olika yrkesroller och kategorier ser vi ett behov av en helhetssyn både inom företag och myndigheter som klarar av både de tekniska, organisatoriska och juridiska perspektiven. Informanternas svar tillsammans med den data som framkommit från teorin leder fram till ett antagande att mer stöd, tydligare riktlinjer och en övergångsperiod från personuppgiftslagen till GDPR hade varit lämpliga. På grund av de något avslappnade attityder som har möts hos informanter vad gäller sanktioner hade myndigheter antagligen tjänat på ett proaktivt arbetssätt där det hade varit tydligt precis vad som gäller med sanktioner och annat. Både intervjusvar och orsakerna till bortfall av informanter gör att indikationer finns att företag inte kommer att vara färdiga med övergången till GDPR när den träder i kraft. De företag som inte är redo kommer behöva arbeta på att nå upp till de krav som GDPR ställer. Resultaten av teori och empiri användes för att skapa en utvärderingsmodell som kommer att kunna hjälpa företag att se hur väl de följer GDPR och kan fungera som ett stöd vid beslutsfattande om förändringar behöver utföras. Vi tror att de frågetecken som återstår

efter att GDPR har trätt i kraft till viss del kommer att rätas ut under det första året, men för de företag som fortfarande har svårigheter hoppas vi att vår utvärderingsmodell kan hjälpa dem att identifiera och stänga gapen mellan nuläge och önskat läge.

6.1 Metoddiskussion och –reflektion

För att kunna studera hur införandet av GDPR påverkar svenska företag anser vi att en kvalitativ metod var det bästa valet. En kvantitativ ansats hade inte resulterat i lika djupgående svar och hade inte lett fram till ett svar på forskningsfrågan då målet inte var att ta fram statistik utan att skapa en större förståelse och kunna skapa en grund att stå på för framtida forskning. Då det i tidigare forskning redan utförts ett flertal enkäter med företag som påverkas av GDPR drogs slutsatsen att vi med ett kvantitativt fokus inte skulle ha bidragit med något nytt till forskningsområdet. Istället gav den kvantitativa datan från tidigare forskning oss en statistisk bakgrund till vår studie. Med hjälp av en kombination av det kvalitativa angreppssättet och ett synsätt inspirerat av hermeneutiken blev det möjligt att få fram nyanserade svar och presenterades en möjlighet att tolka dessa svar för att skapa ny förståelse och på så vis förbättra våra intervjufrågor ytterligare på ett iterativt vis. Varje intervju kan ses som en iteration som gav oss mer information, och denna information gav oss bättre förståelse för forskningsområdet både som helhet och för de olika delarna, enskilt och i kombination med varandra. Som tidigare nämnt är en kvalitativ metod mest lämpad om ämnet inte är särskilt väl utforskat eller om fenomenet fortfarande är under utveckling (Recker 2012) vilket stämmer väl överens med ämnet GDPR.

Trots ett relativt stort bortfall av informanter tycker vi att de svar som har inhämtats tillsammans med teorin tillhandahöll en grund för fortsatt forskning. För att tillföra ytterligare kunskap till forskningsområdet och bidra med något som kan användas vid framtida studier såg vi en möjlighet att använda den information som framkom genom teori och empiri för att själva skapa en utvärderingsmodell. Istället för att enbart konstatera nuläget hos företag jämfört med den information som går att utläsa ur teoretiska källor kunde vi skapa en form av artefakt som kan användas av företag inom vår målgrupp eller i samband med framtida forskning. Denna utvärderingsmodell kan ses som en helhet som är skapad med de olika perspektiven teknik/IT, organisation och juridik som delar. Vi anser att detta styrker vårt hermeneutiska arbetssätt där delar och helhet hjälper till att skapa bättre förståelse för området GDPR.

Som är fallet med alla forskningsmetoder finns det för och nackdelar även med kvalitativa metoder. Recker (2012) beskriver att en kvalitativ metod kan vara svår att arbeta med då både färdigheter och erfarenhet krävs för att som forskare kunna tolka den information som framkommer på ett opartiskt sätt. Författarna av den här uppsatsen har haft tankar kring möjliga resultat, framför allt tidigt i processen, men försökt att inte låta dem påverka hur insamlat material skulle tolkas. Vidare menar Recker (2012) att kvalitativa metoder ofta kan ha problem med reliabiliteten då studierna är så pass beroende av sina sammanhang att det blir svårt att upprepa för en annan forskare. Vi kan förstå och hålla med om denna risk, men med hjälp av ett proaktivt arbetssätt i form av de avgränsningar som har gjorts och de urvalskriterier som har använts har risken minskat. För att säkerställa så god validitet som möjligt i uppsatsen har fokus legat på en grundlig genomgång av tidigare litteratur inom relevanta områden och väl förberedda intervjuer med informanter som innehade god kunskap av GDPR. Många av de steg som tagits för att öka validiteten är inspirerade av Kvale (1995)

som menar att forskningsprocessen hos en studie med intervju som empirisk insamlingsmetod har sju steg. Dessa är tematisering, design, intervjuande, transkribering, analysering, verifiering och rapportering. Varje steg har egna aspekter gällande validiteten. Då fokus låg på att lägga en god teoretisk grund för fortsatt arbete, väl genomtänkta intervjufrågor och informanter som bedömdes kunna ge valida svar stämmer arbetet med den här uppsatsen med flera av de steg som Kvale (1995) beskriver. När det kommer till den teoretiska datainsamlingen var det ett medvetet val att endast välja nyare litteratur. Äldre artiklar kunnat användas för att skapa kontext men valdes bort då sammanhanget även tas upp i nyare artiklar men även innefattar ett GDPR perspektiv. För att få data som hade hög reliabilitet valdes artiklar utifrån ett antal kriterier som skulle säkerställa att de var tillförlitliga. Dessa kriterier var att ett antal nyckelord användes vid sökning av artiklarna, de skulle även vara vetenskapliga och inte vara skrivna före 2010. Den empiriska datainsamlingen utfördes genom intervjuer och för att säkerställa att den data som samlades in höll hög reliabilitet var det tre personer närvarande när intervjuerna utfördes; informanten och två personer som ställde frågor och antecknade. Att vara fler än en person som deltar i intervju minskar risken att informanten misstolkas och enligt Patel och Davidson (2003) blir det lättare att kontrollera reliabiliteten. För att vidare kontrollera reliabiliteten spelades intervjuerna med informant B, C och D in på en mobiltelefon, detta minskar risken för misstolkningar. Informant A avböjde från att bli inspelad vilket gjorde att båda författarna förde anteckningar under samtalet för att säkerställa att data inte misstolkades. Anteckningarna syntetiserades sedan under transkriberingen. Enligt Patel och Davidson (2003) handlar validitet i en kvalitativ studie inte enbart om själva datainsamlingen, utan är en genomgående aspekt i alla delar i forskningsprocessen. För att säkerställa att empirin höll god validitet skickades transkriberingarna från intervjuerna till informanterna som sedan fick bekräfta att inte feltolkningar eller missförstånd skett. Som beskrivit under finns det fördelar och nackdelar med att låta en informant gå igenom transkriberingen då den kan komma att vilja redigera sina svar (Alvehus 2013).

Även då ett fokuserat arbete har skett för att säkerställa validitet och reliabilitet i vår studie har detta varit svårare än om vår studie hade varit kvantitativ. Alvehus (2013) ser problem med begreppen reliabilitet och validitet ur ett kvalitativt perspektiv vilket speglar våra uppfattningar. Alvehus (2013) menar nämligen att begreppen reliabilitet och validitet inte alltid ligger i linje med vad kvalitativ forskning handlar om. Kvale (1995) i sin tur beskriver hur validitet och reliabilitet kan vara svåra att använda inom kvalitativ forskning om den definition som utgås ifrån är smal. Den smala definitionen av validitet handlar om ifall vi har mätt det som vi ville mäta (Kvale 1995). Den bredare definitionen av validitet handlar om ifall vi har undersökt det som vi ville undersöka (Kvale 1995, Alvehus 2013). Kvale (1995) beskriver vidare att det finns många taktiker för att testa och bekräfta kvalitativa fynd, några av dem är triangulering och att väga innebörden och tyngden av olika fynd.

Under skrivprocessen har både fördelar och nackdelar med den valda metoden hittats. En klar fördel är som ovan nämnt att den kvalitativa metoden hjälpt oss att ta fram data som behövdes för att kunna besvara vår forskningsfråga. En nackdel har varit en del svårigheter att säkerställa validitet och reliabilitet då det har krävts mer arbete än om metoden hade varit kvantitativ. Funderingar kring alternativa metoder har förekommit. En av dessa alternativa metoder som även hade kunnat öka validiteten och reliabiliteten av våra fynd var triangulering. Denna metod innebär att data hämtats in på flera olika sätt (Recker 2012)

Generalisering är ett koncept som fungerar mycket bra i kvantitativa studier och lite mindre bra, eller mindre självklart, i kvalitativa studier. Firestone (1993) definierade tre olika typer av generalisering, nämligen statistisk generalisering, analytisk generalisering och översättning från fall till fall, också kallat överförbarhet. I en kvalitativ studie som denna handlar generalisering om att kunna konceptualisera processer och mänskliga erfarenheter genom djupgående analys och därefter abstrahera dessa vilket med ett samlingsnamn kallas för analytisk generalisering. Enligt Firestone (1993) handlar generalisering för att stödja ett koncept om att hitta bevis som stödjer konceptet. I analytisk generalisering ligger tonvikten på analys och tolkning (Polit & Beck 2010). Tillvägagångssättet i den här studien var att samtidigt som de utförda intervjuerna transkriberades och bearbetades tolkades de och paralleller drogs både mellan de olika svar som inkommit från olika informanter och mellan intervjusvaren och den teoretiska grund som insamlats. Härigenom var det möjligt att utesluta svar som stack ut på olika vis. Dessa svar hade gjort det svårt att applicera svaren på en större massa och var inte användbara i ett generaliseringssyfte. För studiens skull är dessa svar ändå med i slutprodukten eftersom vår urvalsgrupp inte blev så stor vilket gjorde att dessa resultat ändå kunde vara av intresse för den tilltänkta målgruppen.

Några punkter som är viktiga när det gäller analytisk generalisering är att det är viktigt att sluta samla in data först när en mättnad har uppnåtts, istället för vid aha-ögonblick eller av bekvämlighet (Polit & Beck 2010). Då intervjuerna bearbetades märktes relativt snabbt att de olika informanterna relativt snabbt uppnådde en gemensam syn på ämnena som togs upp under intervjuerna vilket gjorde att beslutet togs att fler informanter inte nödvändigtvis skulle behövas, även om det hade kunnat stärka vår analys. När det skrivs om replikering, eller möjligheten att återskapa, kan detta göras på olika nivåer så som beskrivs av Polit och Beck (2010). En väldefinierad målgrupp och tydliga avgränsningar som utförts i den här uppsatsen gör att det rent praktiskt borde vara lätt att återskapa förutsättningarna för den här studien. Sett till mättnadsgrad, som är ett annat sätt att mäta hur väl en studie kan återskapas, hade det varit möjligt att tillfråga ytterligare potentiella respondenter att delta. Som nämnt ovan anses dock att mättnad av svar har uppnåtts. Polit och Beck (2010) menar vidare att urvalet påverkar möjligheten till generalisering, och bekvämlighetsurval påverkar det särskilt dåligt. Två av respondenterna i den här studien har tillkommit till viss del genom bekvämlighetsurval men hade inte tillfrågats om de inte uppfyllde de övriga kriterierna som fanns vad gällde den tilltänkta målgruppen och avgränsningarna.

Vi menar att generalisering är möjlig tack vare ett tydligt urval av informanter och den mättnad som uppnåddes vad gäller de mottagna svaren på intervjufrågorna. Med aspekten överförbarhet för ögonen anses att studien är överförbar, så länge som kriterierna för målgrupp och avgränsning följs. Eftersom GDPR är ett ämne som kommer gälla för alla som hanterar personuppgifter bör liknande resultat uppnås även inom andra sektorer än det privata näringslivet.

6.2 Vidare forskning

Eftersom GDPR ännu inte tillämpas ser vi möjligheter till vidare forskning inom områden som tekniska lösningar, hur organisationer ska arbeta med förtroendeskapande och om en ny form av märkning (exempelvis privacy seal) kommer att hjälpa. En annan möjlighet för vidare forskning är hur företag som arbetar med datainsamling i stora volymer kommer att arbeta i fortsättningen. Kommer det ske en stor förändring i hur detta arbetet utförs då samtycke krävs eller kommer ett sätt att kringgå detta att användas?

Vi snuddade vid ämnet data valorisation i vår forskningsöversikt, där Perera et al. (2017) föreslog sätt för företag att kompensera individer på olika sätt för att få tillstånd att använda deras data för affärssyften. När GDPR trätt i kraft kan det finnas ett intresse i att undersöka detta ämne närmare. Främst när det gäller hur företag väljer att få kunder till att dela med sig av sin data men även från individen perspektiv, hur denne ser på att dela sin data och vad som krävs för att göra det.

Andra områden att utforska är hur myndigheter som Datainspektionen ska hantera företag som inte följer den nya lagstiftningen. Detta är något som vi har fått indikationer på, både genom intervjusvar och genom kontakt med informanter som valde att inte delta. Av intresse är även vad för typ av förseelser som kommer att ge böter i 4 %-klassen. Kommer företag få en chans att rätta till sitt fel först, eller en varning vid första förseelsen? Vad kommer det att finnas för graderingar vad gäller storlek av sanktioner och hur kommer detta att kontrolleras?

Denna uppsats utforskade området kring rättigheten med dataportabilitet men det fanns inga tydliga tillvägagångssätt fastställda av informanternas företag än. Det är dock något som skulle gå att forska mer vidare om, hur ska användare hantera sin data om de väljer att “hämta ut” den? Sen kan det vara av intresse att undersöka om det finns några användningsområden för information som hämtats ut på detta sätt från företag. Kommer det att finnas ett värde i den data som en individ samlat på sig från alla de företag och tjänster som denne använt? I så fall, hur kan denna information skapa värde både för ett företag och för personen som informationen tillhör?

Referenser

Akter, S. & Wamba, S.F. (2016). Big data analytics in E-commerce: a systematic review and agenda for future research, *Electronic Markets*, vol. 26, no. 2, ss. 173-194.

Alvehus, J. (2013) *Skriva uppsats med kvalitativ metod: En handbok.* Stockholm: Liber AB.

Alvesson, M. & Sköldberg, K., (2008). *Tolkning och reflektion : vetenskapsfilosofi och kvalitativ metod*, Lund: Studentlitteratur.

Arvidson, K. Bladh, P. (2017). *Quasi identifiers and the challenges of anonymising data Part 1.* https://www.basalt.se/blogg/quasi-identifiers-challenges-anonymising-data-part-1/ [2017-04-17]

Backman, J. (2016). *Rapporter och uppsatser* 3., [rev.] uppl.., Lund: Studentlitteratur.

Chen, H. & Yan, Z. (2016). Security and privacy in big data lifetime: A review. ss. 3.

Collins, K. Egner, M. (2017). *GDPR: The Time To Act Is Now*. https://www.accenture.com/t20170409T005113__w__/us-en/_acnmedia/PDF-49/Accenture-Webscale-General-Data-Protection-Regulation-Accenture.pdf [2017-04-17]

Datainspektionen (2017). *Introduktion till dataskyddsförordningen.* http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/dataskyddsdagen/ [2017-04-06]

Datainspektionen (2017) *Personuppgiftslagen* http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/ [2017-04-26]

Dickie, N., Yule, A. (2017). Privacy by design prevents data headaches later, *Strategic HR Review*, Vol. 16 Issue: 2, ss.100-101 DOI: 10.1108/SHR-01-2017-0008

Dell (2016). *GDPR: Perceptions and Readiness A Global Survey of Data Privacy Professionals at companies with European Customers.* http://www.eurocloud.fr/wp-content/uploads/2016/10/gdpr.pdf [2017-04-17]

Engels, B. (2016). Data portability among online platforms. *Internet Policy Review*, 5(2). DOI: 10.14763/2016.2.408

Eriksson, L.T. & Weidersheim-Paul, F. (2011). *Att utreda forska och rapportera* 9. uppl.., Malmö: Liber.

Esaiasson, P., 2017. *Metodpraktikan : konsten att studera samhälle, individ och marknad* 5., [rev.] uppl.., Stockholm: Norstedts juridik.

EUR-Lex (2014). *Protection of Personal Data* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012 [2017-04-13]

EUROPA (2017) *The EU in Brief* https://europa.eu/european-union/about-eu/eu-in-brief_en [2017-04-26]

European Data Protection Supervisor (2017). *The History of the General Data Protection Regulation* https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [2017-04-13]

Europeiska Kommissionen (2015) Special Eurobarometer 431 Data protection.
DOI: 10.2838/552336
http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Europeiska Kommissionen (2017) *Tillväxt - Inre marknaden, industri, entreprenörskap samt små och medelstora företag.*
http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_sv [2017-05-23]

Firestone, W.A.A., 1993. Alternative Arguments for Generalizing From Data as Applied to Qualitative Research. *Educational Researcher*, 22(4), ss.16–23.

Fortinet (2014). *Fortinet Reveals "Internet of Things: Connected Home" Survey Results*. http://investor.fortinet.com/releasedetail.cfm?releaseid=855992 [2017-04-05]

Gartner (2015). *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015.* http://www.gartner.com/newsroom/id/3165317 [2016-11-25]

Holme, I.M., Solvang, B.K. & Nilsson, B. (1997). *Forskningsmetodik : om kvalitativa och kvantitativa metoder* 2., [rev. och utök.] uppl.., Lund: Studentlitteratur.

ISO (1998). *ISO 9241-11:1998(en) Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*. https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-1:v1:en [2018-01-23]

Kieselmann, O., Kopal, N., Wacker, A. (2015) *A Novel Approach to Data Revocation on the Internet*
DOI: 10.1007/978-3-319-29883-2_9 [2017-04-10]

Kvale, S., 1995. The Social Construction of Validity. *Qualitative Inquiry*, 1(1), ss.19–40.

Mayfield, K. (2016). Pseudonymisation: a 20-year-old idea never seemed so timely, *Journal of Direct, Data and Digital Marketing Practice*, vol. 17, no. 4, ss. 222-226.

McStay, A. (2016) Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy), *Big Data & Society*, vol. 3, no. 2.

Mitchell, A. (2016). *GDPR: Evolutionary or revolutionary?*
Journal of Direct, Data and Digital Marketing Practice (2016) 17,
217–221. DOI:10.1057/s41263-016-0006-9 [2017-04-10]

Nielsen, J. (1995). *Ten usability heuristics.*
https://www.nngroup.com/articles/ten-usability-heuristics/ [2018-01-21]

Nyrén, O., Stenbeck, M. & Grönberg, H. (2014) The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research, *European Journal of Epidemiology*, vol. 29, no. 4, ss. 227-230.

Näringsdepartementet (2016) *Nyindustrialiseringsstrategi för Sverige.* Stockholm: Näringsdepartementet http://www.regeringen.se/48f359/contentassets/869c75f458fc4585ab4ec8c13b250a07/informationsmaterial-smart-industri---en-nyindustrialiseringsstrategi-for-sverige [2017-04-26]

O'Brien, R. (2016) Privacy and security. *Business Information Review*, vol. 33(2), ss. 81–84.

Patel, R. & Davidson, B. (2003). *Forskningsmetodikens grunder : att planera, genomföra och rapportera en undersökning* 3., [uppdaterade] uppl.., Lund: Studentlitteratur.

Patton, M.Q., (2002). *Qualitative research & evaluation methods* 3. ed., London: SAGE.

Perera, C., Wakenshaw, S. Y. L., Baarslag, T., Haddadi, H., Bandara, A. K., Mortier, R., Crabtree, A., Ng, I. C. L., McAuley, D., and Crowcroft, J. (2017) Valorising the IoT Databox: creating value for everyone. *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 1, ss. e3125-n/a. DOI: 10.1002/ett.3125.

Polit, D.F. & Beck, C.T., 2010. Generalization in quantitative and qualitative research: myths and strategies. *International journal of nursing studies*, 47(11), ss.1451–8.

Recker, J., 2012. *Scientific Research in Information Systems : A Beginner's Guide*, Berlin/Heidelberg: Springer.

Ricœur, P. & Thompson, J.B., 1981. *Hermeneutics and the human sciences : essays on language, action and interpretation*, Cambridge: Cambridge U.P.

Rodrigues, R., Barnard-Wills, D., De Hert, P. & Papakonstantinou, V. (2016). The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR, *International Review of Law, Computers & Technology*, vol. 30, no. 3, ss. 248-270. http://dx.doi.org/10.1080/13600869.2016.1189737

Rudman, R., Sexton N. (2016). *The Internet of Things.* Accountancy Sa. ss. 22-23. http://search.proquest.com/docview/1794510817?pq-origsite=summon [2017-04-13]

Schartum, D.W. (2016). Making privacy by design operative, *International Journal of Law and Information Technology*, vol. 24, no. 2, ss. 151-175. https://doi.org/10.1093/ijlit/eaw002

Schulz, M. Hennis-Plasschaert, J.A. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* http://eur-lex.europa.eu/eli/reg/2016/679/oj [2017-04-17]

Sveriges Riksdag (1973). *Datalag (1973:289)* http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289 [2017-04-26]

Sveriges Riksdag (1998). *Personuppgiftslag (1998:204)* https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204 [2017-04-26]

Trost, J. (2005). *Kvalitativa intervjuer* 3. uppl.., Lund: Studentlitteratur.

TRUSTe. (2015). *Preparing for the EU General Data Protection Regulation.* https://iapp.org/media/pdf/resource_center/TRUSTe_GDPR_Report_FINAL.pdf [2017-04-17]

Zetterlund, A. (1997). *Utvärdering och folkbibliotek : en studie av utvärderingens teori och praktik med exempel från folkbibliotekens förändrings- och utvecklingsprojekt*, Borås : Göteborg: Valfrid ; Avd. för biblioteks- och informationsvetenskap, Univ.

Ziegeldorf, J.H., Morchon, O.G. & Wehrle, K., 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, 7(12), ss.2728–2742.

Bilagor

Bilaga 1 - intervjuguide

En intervjuguide användes som fokuserade på ett antal områden med tillhörande begrepp och aspekter som var kopplade till området som bedömts vara relevanta baserat på insamlad teori.

Tekniska frågor:

- Personlig data, hur stor utsträckning? Det intressanta var att ta reda på vad för slags personlig data som samlas in, hur den hanteras och hur dess livscykel i informantens system ser ut.
- Dataportabilitet; Hur kommer den intervjuades företag att hantera denna rättighet ur ett tekniskt perspektiv?
- Radering av personlig data: Hur kan den intervjuades företag vara säkra på att all personlig data om en individ är raderad ur alla system? hur garanterar de att deras samarbetspartners tar bort den data de hanterar i rollen som personuppgiftsbiträde?
- Ändrade processer och rutiner; i vilken utsträckning påverkas processer och rutiner med den nya dataskyddsförordningen?

Organisatoriska frågor:

- Medvetenhet och stöd inom verksamheten för övergången till GDPR; hur länge har arbetet med övergången pågått och vad kommer anställda att utbildas om när det gäller hantering av persondata?
- Data Protection Officer (DPO); kommer den intervjuades företag att tillsätta denna rollen?

Juridiska frågor:

- General Data Protection Regulation (GDPR); Hur arbetar den intervjuades företag med se till att de kommer vara förenliga med de nya reglerna?
- Hur avtal, försäkringar och samarbete med kunder och andra företag kommer att hanteras med GDPR.

Kopplat till dessa områden fanns det frågor som mer i detalj sökte svar på vissa aspekter inom området. Utformningen av frågorna var av en medelgrad av standardisering. I kontrast till den valda standardiseringsnivån beskriver Trost (2007) att en hög grad av standardisering innebär att frågorna och situationen är samma för alla informanter. Frågorna ställs alltid i samma följd och inga förklaringar på frågor ges till en informant om den inte förklaras för alla. En låg grad av standardisering innebär att frågorna anpassas efter informanten och ordningsföljden är inte viktig utan kan styras av den intervjuade. Detta leder till en större variation med följdfrågor baserade på tidigare svar. Med detta som grund var en medelgrad av standardisering det som var mest lämpligt. Ämnesområdet är så pass nytt och det var av vikt att intervjuerna ledde till så utförliga svar som möjligt. De frågor som vi behövde ha svar på var därför tydligt formulerade men det fanns en viss flexibilitet i hur följdfrågor kunde utvecklas då intervjuerna bedrevs på olika företag där det fanns olika behov i hur processer behövde ändras för att motsvara de krav som GDPR har. Baserat på den empiri som en intervju resulterar i så justeras frågorna inför nästa intervju. Detta för att på ett mer flexibelt sätt kunna anpassa frågorna för att få den empiri som är mest relevant.

Trost (2007) tar upp termen *strukturerad* i koppling till intervjufrågor och beskriver att frågorna utformas med fasta svarsalternativ. Trost (2007) beskriver vidare hur termen

ostrukturerad innebär motsatsen, det vill säga öppna svarsalternativ där informantens svar kommer att ligga till grund för den struktur som frågan får.. En hög strukturering innebär att intervjun som helhet håller sig till ett område i vad som ska undersökas och hur frågorna formuleras. En låg strukturering kan innebära att flera områden undersöks samtidigt (Trost 2007). I denna uppsats fall var frågorna ostrukturerade men den övergripande utformningen av tillvägagångssättet var av en hög strukturering. Baserat på detta kan intervjuerna som gjordes klassas som semi-strukturerade.

Fokus på de enskilda frågornas utformning var att ta fram teoretiska frågor snarare än analytiska frågor. Trost (2007) menar att analytiska frågor inte bör ställas till informanten utan snarare sparas till att användas för tolkningar och analyser av den insamlade informationen. Vidare anser Trost (2007) att frågor om tankar och upplevelser inte heller ska ställas utan detta besvaras genom att ställa konkreta frågor om aktiviteter, beteenden och handlingar.

Vid första kommunikationen och vid intervjuns start framfördes att allt som togs upp i intervjun skulle vara strikt konfidentiellt i transkribering och uppsats. Med andra ord försäkrades informanten om att det inte skulle framgå någon information som på något sätt unikt skulle kunna vara identifierade. Enligt Trost (2007) är det upp till den som intervjuar att på ett adekvat sätt se till att den intervjuade är anonymiserad i avrapporteringen. Det står fritt fram för den som deltagit i en intervju att berätta detta för sin omgivning men för den som var ansvarig eller genomförde intervjun får det inte framkomma vem individen är som deltagit. För att underlätta för läsaren har informanterna pseudonymiserats i empirikapitlet.

Det är viktigt att en intervju genomförs på en plats där informanten känner sig trygg och bekväm (Trost 2007). Vid kontakt med de tillfrågade informerades det att det fanns tillgängliga grupprum på Högskolan i Borås som kunde bokas för att intervjun skulle kunna genomföras i en lugn miljö. Alla informanterna valde att genomföra intervjun på deras respektive arbetsplats. Om det inte hade varit möjligt att träffas för en intervju ansikte mot ansikte föreslogs även möjligheten att genomföra en telefonintervju eller att få frågorna skickade via e-mail. Detta var det dock ingen som valde.

University of Borås is a modern university in the city center. We give education programs and courses in business administration and informatics, library and information science, fashion and textiles, behavioral sciences and teacher education, engineering and health sciences.

At the **Department of Information Technology,** we have focused on the students' future needs. Therefore, we have created programs in which employability is a key word. Subject integration, wholeness and contextualization are other important concepts. The department has a closeness, both between students and teachers as well as between industry and education.

Our **courses and programs** with a major in informatics are centered around basic concepts as system development and business development. In our wide range of specializations there is everything from programming advanced systems, analyze the needs and requirements of businesses, to conduct integrated IT and business development, with the common purpose of promoting good use of IT in enterprises and organizations.

The department is carrying out IT-related **research** within the university's research area called Business and IT. In terms of field, the research activities are mainly within **computer and systems science**. Particular areas of focus are **data science** and **information systems science**. Both scientifically and professionally-oriented research are performed, which among other things is manifested through that research is often conducted based on domain specific needs of business and government organizations at local, national and international arena. The professionally-oriented research is also often manifested through our participation in the Swedish Institute for Innovative Retailing (SIIR), which is a research center at the University with the aim of contributing to commerce and society with the development of innovative and sustainable trade.

UNIVERSITY
OF BORÅS

VISITING ADDRESS: JÄRNVÄGSGATAN 5 · POSTAL ADDRESS: ALLÉGATAN 1, SE-501 90 BORÅS
PHONE: + 46 33 435 40 00 · E-MAIL: INST.HIT@HB.SE · WEB: WWW.HB.SE/HIT