Examensarbete

HÖGSKOLAN I SKÖVDE

ANPASSNINGAR TILL GDPR HOS FÖRETAG

En genomgång av tekniska förändringar som genomförs inför GDPR

ADJUSTMENTS BY COMPANIES TO GDPR

A review of technical changes implemented for GDPR

Examensarbete inom huvudområdet informationsteknologi med inriktning mot nätverks- och systemadministration G2E 22,5 Högskolepoäng IT610G, Vårtermin 2018

Lukas Nord
2018-06-04

Handledare: Johan Zaxmy
Examinator: Rose-Mharie Åhlfeldt

Sammanfattning

Den 25e maj 2018 ersätts personuppgiftslagen (PuL) med den nya dataskyssförordningen (GDPR) som skärper till och stramar åt kraven som ställs på företag och organisationer som behandlar personuppgifter. Det finns dock flera saker som är densamma mellan PuL och GDPR. Syftet med den här undersökningen är att försöka ta reda på hur förberedda organisationer är inför GDPR genom att undersöka vilka tekniska förändringar de har behövt införa för att uppfylla de nya kraven. Genom att utföra en kvalitativ intervjustudie på organisationer som behandlar personuppgifter i enlighet med PuL och GDPR. De utvalda företagen är sådana som har möjlighet att kartlägga konsumtionsvanor kopplat till konsumenten genom t.ex. en kundklubb. För att uppfylla syftet och svara på forskningsfrågan används två delfrågor, vad de har för tekniska lösningar under PuL och vad de har behövt förändra inför GDPR. Baserat på dessa och den bakomliggande teorin har ett intervjuunderlag tagits fram för att försöka få svar på dessa frågor. Utöver intervjuerna analyseras även samtyckesavtal för att se om det går att dra några slutsatser baserat på dessa om de har tekniska lösningar för att uppfylla GDPR. Det förväntade resultatet som fanns vid undersöknings start var att organisationer inte har det som krävs för PuL och ännu mindre det som krävdes för GDPR, de bör alltså ha varit tvungna att införa nya tekniska lösningar.

Resultatet från undersökningen visar att det är en väldig skillnad på hur organisationerna har jobbat med PuL, och att enbart enstaka har använt sig av kryptering för att skydda uppgifterna medans näst intill alla har jobbat med anonymisering. Inför GDPR går organisationerna lite åt samma håll då de flesta uppger att de jobbar med kryptering, åtkomstkontroller och anonymisering. Samma sak gäller dataportabilitet och säkerhetskopieringssystem för att undvika att bortglömda konsumenter återställs från säkerhetskopior, då majoriteten av organisationerna uppger att de inte kommer ha stöd för det. Något som även alla organisationer uppgav var att de inte kommer att vara färdiga med anpassningen och att en stor del av arbetet innebär processer och rutiner.

Nyckelord: GDPR, Personuppgiftslagen, PuL, Tekniska lösningar, Personuppgifter

Abstract

May 25th, 2018, the Personal Data Act (PuL) will be replaced by the new General Data Protection Regulation (GDPR), which will tighten the requirements placed on companies and organizations that are processing personal data. However, many things will remain the same between PuL and GDPR. The purpose of this study is trying to find out how prepared the organizations in question are facing the GDPR, by investigating which technical changes they should introduce to meet the new requirements. By performing a qualitative interview study on organizations that are processing personal data in accordance with PuL and GDPR. The chosen companies have the possibility to map consumption habits linked to the consumer, for example by a loyalty club. To satisfy the purpose of this study and answer the research question, two sub questions are used, what technical solutions they have used for PuL and what changes they have introduced for GDPR. Based on these two sub questions and the background theory, an interview background has been developed trying to answer these questions. In addition to the interviews the consent agreement will be analyzed, to see if any conclusions about what technical solutions they have implemented to fulfill GDPR can be drawn. The hypotheses which was at the start of the survey were that the organizations don't have what is required to fulfill PuL and even less of what is required to fulfill GDPR, they should have had to introduce new technical solutions.

The result from the survey shows a big difference in how organizations have worked with PuL, and only a few of them have used encryption to protect the data and with almost all of them have worked with anonymization. When working with GDPR, the organizations are working in the same direction where all of them says that they are working with encryption, access controls and anonymization. The same applies to data portability and backup systems to avoid that forgotten consumers are recovered from backups. One thing that all organizations say is that they will not be ready with the adjustments and that a large proportion of the work involves processes and routines.

Keywords: GDPR, Personal Data Act, PuL, Technical solutions, Personal data

Innehållsförteckning

1 Inledning

Verksamheters information om deras kunder ökar mer och mer i takt med digitaliseringen och under ett tal 2009 jämfördes personuppgifter med olja (Kuneva, 2009; Spiekermann, Acquisti, Böhme, & Hui, 2015). Att införandet av *General data protection regulation* (GDPR), dataskyddsförordningen på svenska, har blivit ett hett fenomen inom svenska företag och organisationer de senaste åren är kanske inte så konstigt då nästintill alla kommer att påverkas (Hert, 2016). GDPR kommer gälla från och med 25 maj 2018 inom hela den Europeiska unionen. GDPR kommer även att ersätta det nuvarande dataskyddsdirektivet, 95/46/EG, vars syfte är att skydda personers rättigheter när personuppgifter behandlas (Datainspektionen, 2018d). I och med införandet av GDPR skärps de nuvarande kraven på behandling av personuppgifter (Datainspektionen, 2017b).

Då dataskyddsdirektivet enbart varit ett direktiv, har varje nation implementerat en egen tolkning, vilket skapat en situation där lagen divergerar mellan medlemsstaterna. Anpassningsproblemet som funnits försvinner i och med införandet av GDPR, eftersom att GDPR är en förordning och blir då direkt tillämpad som lag i alla medlemsstater (Mittal, 2017). Ett annat problem med dataskyddsdirektivet är att den digitala utvecklingen har stuckit iväg vilket resulterar i eftersläpningar mellan säkerhetspolicys och den digitala revolutionens papperslöshet (Krystlik, 2017).

Även om införandet och anpassningen till GDPR är aktuellt just nu, och organisationer jobbar febrilt med att anpassa sin verksamhet till de nya kraven som skärps, läggs till och förändras, har flera av kraven i den nya lagen redan funnits i Sverige sedan 1998 då dataskyddsdirektivet infördes i form av personuppgiftslagen (PuL) (Mittal, 2017).

Två av sakerna som kan ha bidragit till att GDPRs införande har blivit så stort jämfört med PuL är de nya höga sanktionsavgifterna som kan straffa organisationer som inte lever upp till kraven (Ryz & Grest, 2016) samt att det i praktiken inte kommer vara någon individ som inte blir påverkad av GDPR (Hert, 2016). Ett problem med PuL är att de som inte lever upp till lagstiftningen inte får kännbara straff, då bristen på anmälningar som lätt till åtal är väldigt få (Poullet, 2006; Svanfeldt, 2006; Sveriges radio, 2013).

Syftet med studien är att genom en kvalitativ intervjustudie undersöka vilka tekniska system som organisationer har behövt applicera i sin verksamhet för att uppfylla kraven för PuL och deras eventuella förändringar inför GDPR. Eftersom GDPR definierar explicita säkerhetsåtgärder och andra krav som verksamheter behöver uppfylla bör organisationer utvärdera och införa nya tekniska lösningar. Användandet av en intervjustudie bör passa bra då området kan ses på fler olika sätt, vilket gör att olika organisationer antagligen ger olika svar. Det kan därför bli svårt att precisera exakta frågor som t.ex. en enkät hade behövt (Hedin, 1996).

2 Bakgrund

I följande kapitel kommer en djupare bakgrundsförståelse att presenteras för att kunna förstå den fortsatta studien. Först kommer de olika delarna av PuL och GDPR presenteras för att

skapa förståelse för dess likheter och skillnader. Därefter presenteras olika tekniska implementationer som en organisation kan beröras av i och med införandet av GDPR.

2.1 Personuppgiftslagen

Personuppgiftslagen (PuL) är en svensk lag som infördes år 1998 med syfte att se till att personers integritet inte kränks vid behandling av personuppgifter (SFS 1998:204, 1998). Begreppet ”behandling” omfattar flera olika saker, t.ex. insamling, registrering, lagring, bearbetning, spridning och utplåning av personuppgifter (Datainspektionen, 2018h). PuL baseras på Europeiska Unionens dataskyddsdirektiv, 95/46/EG, som kom år 1995. Ett direktiv är ett dokument som berättar för medlemsnationerna vilka mål de ska uppnå, men inte exakt hur de ska gå tillväga (Europeiska unionen, 2018). Cate (1995) skriver i en artikel att personuppgifter enbart får behandlas inom ramen för det syfte som de samlades in för och får inte behandlas i en identifierbar form under längre tid än vad som krävs för att uppfylla behandlingens syfte.

De personuppgifter som lagen omfattar är de som utsätts för helt eller delvis automatiserad behandling, samt de personuppgifter som är tänkta att ingå i ett strukturerat material. Ett strukturerat material är t.ex. databaser, ärendehanteringssystem eller andra system som underlättar indexering och sökning efter uppgifter (SFS 1998:204, 1998). Det finns dock undantag från PuL, vilka är att om en annan lag motsäger vad som bestäms i PuL är det den andra lagen som ska gälla. Det innebär att om lagar inom t.ex. skatteförvaltning, socialtjänst och polismyndighetens arbete talar om hur de får behandla personuppgifter så är det de som gäller. Andra undantag från PuL är att den inte gäller vid hantering av personuppgifter för privat bruk, samt att det finns undantag i offentlighetsprincipen och tryck- och yttrandefriheten (Datainspektionen, 2018d).

Ostrukturerad behandling är, tillskillnad mot strukturerad behandling, den behandling som inte underlättar sökning i uppgifterna som t.ex. personuppgifter som behandlas i ett ordbehandlingsprogram, ljud och bildupptagningar, e-postmeddelande och löpande text på internet (Datainspektionen, 2018g). Om personuppgifter samlats in med syfte att de ska ingå i ett ostrukturerat material finns ett undantag i PuL som säger att personuppgifter får behandlas i ostrukturerat material så länge som det inte är integritetskränkande mot den registrerade (SFS 1998:204, 1998). Enligt Datainspektionen (2018g) innebär det att så länge behandlingen inte är kränkande får den genomföras i ostrukturerat material, men de påpekar även att en bedömning bör göras för att veta vilken typ av behandling som inte är kränkande.

Ett centralt begrepp inom personuppgiftsbehandling är personuppgiftsansvarig som är en juridisk person, dvs. aktiebolag, stiftelse eller myndighet. Definitionen av personuppgiftsansvarig är enligt 3 § i personuppgiftslagen ”Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter” (Datainspektionen, 2018c; SFS 1998:204, 1998). Om den personuppgiftsansvariga anlitar en fysisk eller juridisk person utanför den egna organisationen benämns den anlitade som personuppgiftsbiträde. Ett personuppgiftsbiträde behandlar personuppgifter för den personuppgiftsansvariges räkning och definieras i § 3 i personuppgiftslagen. Det måste alltid

finnas ett skriftligt avtal mellan en personuppgiftsansvarig och dess personuppgiftsbiträden (Datainspektionen, 2018c).

2.1.1 Personuppgifter enligt PuL

En personuppgift enligt PuL definieras som ”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet” i § 3 i personuppgiftslagen. Inom personuppgifter finns det även kategorin ”känsliga personuppgifter”. De känsliga personuppgifterna är personuppgifter som avslöjar följande,

- Ras och etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Hälsa och sexualliv

Dessa uppgifter är förbjudna att behandla såvida inte särskilda undantag uppfylls. De undantagen är om t.ex. samtycke givits, om uppgifterna har gjorts offentliga av den berörda personen eller om det är nödvändiga uppgifter för att den personuppgiftsansvarige ska kunna uppfylla dennes skyldigheter. Uppgifter om hälsa- och sjukvård får behandlas om de är nödvändiga för förebyggande, ställande av medicinska diagnoser samt om vård eller behandling ges. Känsliga uppgifter om politisk, religiös eller filosofisk ståndpunkt samt fackligt engagemang får behandlas av ideella organisationer om det är av betydelse och inom ramen för deras verksamhet. Känsliga personuppgifter får även i vissa fall behandlas vid forskningsändamål om forskningsprojektet har genomgått och blivit godkänd vid en etikprövning (SFS 1998:204, 1998).

2.1.2 Samtycke i PuL

Grundbulten i behandlingen av personuppgifter är att det bara är tillåtet om den registrerade personen ifråga har lämnat sitt godkännande, dvs. ett samtycke till behandlingen. Vid insamlandet av samtycket, som ska vara individuellt, frivilligt och särskilt, ska den registrerade få tillräckligt med information om den tänkta behandlingen. Det innebär att det ska vara den registrerade som själv lämnar samtycket, att det ska vara frivilligt för den registrerade att lämna samtycket och att samtycket ska vara för ett specifikt ändamål och inte generellt. Den registrerade ska ha möjlighet att ta ställning till behandlingen innan denne godtar den. Ett samtycke som samlas in via ett antagande är inte ett giltigt insamlat samtycke enligt personuppgiftslagen (Datainspektionen, 2018f).

Vid insamlande av känsliga personuppgifter måste den personuppgiftsansvarige välja ett sätt att samla in samtycket på som är extra uttryckligt, vilket innebär att samtycket ska visa den registrerades vilja till insamlingen tydligt (Datainspektionen, 2018f).

Som tidigare nämnts är grunden i PuL att personuppgifter enbart får behandlas om personen i fråga har lämnat sitt samtycke. Det finns dock ett par punkter i lagen som ger undantag från samtyckeskravet vilka är,

- om det finns ett avtal där personuppgifter behövs för att avtalet ska gå att uppfylla,
- om det krävs för att den personuppgiftsansvariga ska kunna följa de rättsliga skyldigheter denne har,
- om den personuppgiftsansvarige behöver personuppgifterna för att skydda den registrerades intressen,
- om det finns arbetsuppgifter av allmänt intresse som måste gå att utföra,
- om en arbetsuppgift inom myndighetsutövning kräver att personuppgifterna behandlas,
- om den personuppgiftsansvarigas ändamål har ett intresse som väger tyngre än den registrerades intresse för skydd av den personliga integriteten.

Eftersom att stora delar av behandlingen av personuppgifter grundar sig på samtycke ifrån den registrerade, kan den registrerade när som helst återkalla det samtycke som givits. Den personuppgiftsansvariga har då inte längre rätt att behandla uppgifter om personen ifråga (SFS 1998:204, 1998).

Personnummer får behandlas utan samtycke om det motiveras med hänsyn till vilket ändamål uppgiften behandlas i, hur viktigt det är med en korrekt identifiering eller om det finns andra skäl värda att beakta (SFS 1998:204, 1998).

2.1.3 Information till den registrerade

När en person lämnar personuppgifter för behandling ska den registrerade få information om den behandling som kommer att ske. Detta gäller även om personuppgifterna har tagits in via någon annan källa med undantag om avsikten är att lämna ut uppgifterna till tredje man, dvs. en person som under den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar har rätt att behandla personuppgifter, behöver information till den registrerade ske först vid utlämnandet. Undantaget till att lämna ut information om uppgifterna som inhämtats från en annan källa är om det finns motstridiga bestämmelser i annan lag samt om det anses vara omöjligt eller att arbetsinsatsen anses vara för stor (SFS 1998:204, 1998).

Den informationen som den registrerade ska få vid insamlingen av uppgifterna ska innehålla,

- Den personuppgiftsansvarigas identitet,
- ändamålet med behandlingen,
- samt all annan information som den registrerade behöver för att ha möjlighet att ta tillvara på de rättigheterna som denne har vid behandlingen.

Den övriga informationen kan innehålla saker som uppgifter om mottagarna av ens uppgifter, vilka skyldigheter den personuppgiftsansvarige har att lämna ut vilka uppgifter som behandlas om den registrerade samt vilka rättigheter den registrerade har till rättelse av felaktiga uppgifter (SFS 1998:204, 1998).

Utöver att den registrerade ska få information om behandlingen innan insamlingen av personuppgifter har den registrerade enligt PuL rätt att kostnadsfritt en gång per kalenderår begära ut vilken information som en personuppgiftsansvarig har och behandlar om den registrerade som begär informationen. Informationen ska lämnas ut skriftligen och ska

innehålla vilka uppgifter som behandlas och dess ändamål, varifrån uppgifterna är inhämtade och till vilka mottagare som uppgifterna kan komma att lämnas ut till (SFS 1998:204, 1998).

Om en personuppgiftsansvariga omfattas av sekretess eller tystnadsplikt får denne enligt de bestämmelser som finns i offentlighets- och sekretesslagen (2009:400) avstå från att lämna ut uppgifter till den registrerade (SFS 1998:204, 1998).

2.1.4 Rätten till rättelse

Om den registrerade upptäcker att det finns fel i de uppgifter som behandlas av en personuppgiftsansvarig har denne rätt till att begära rättelse, blockering eller radering av uppgifterna. Det gäller uppgifter som inte har behandlats enligt de bestämmelser som finns i PuL. Om personuppgifterna har lämnats ut till tredje man har den personuppgiftsansvarige skyldighet att meddela om sådana förändringar till denne (SFS 1998:204, 1998). I direktivet som PuL baseras på står det att den registrerade ska ha möjlighet att få uppgifter borttagna innan de överförs till en tredje part eller används för direkt marknadsföring (Cate, 1995).

2.1.5 Automatiserade beslut

Ett automatiserat beslut innebär att en process automatiskt tar beslut om den registrerade baserat på fördefinierad logik. Den registrerade har rätt att inte bli föremål för sådana beslut om de är ogynnsamma och behandlar personliga aspekter som t.ex. beteende, kreditvärdighet och tillförlitlighet (Cate, 1995). I PuL innebär det att den registrerade kan begära att istället få beslutet fattat av en person. Den registrerade har även rätt att få reda på vilken logik och på vilka uppgifter det automatiserade beslutet är fattat (SFS 1998:204, 1998).

2.1.6 Säkerhet i PuL

I EU direktivet finns det grundläggande krav på säkerhet där personuppgifter ska skyddas mot oavsiktlig och/eller olaglig förändring samt mot obehörig modifiering och tillgång av uppgifterna (Cate, 1995). Säkerhetsåtgärder ska implementeras enligt PuL för att uppnå en lämplig säkerhetsnivå genom att ta hänsyn till vilka tekniska möjligheter som finns, kostnad för införande, vilka risker som finns med behandlingen samt vilken känslighetsgrad uppgifterna har. Säkerhetsåtgärder kan vara både tekniska och organisatoriska. Om ett personuppgiftsbiträde används av en organisation ska den personuppgiftsansvarige se till att biträdet har rätt kompentens att genomföra åtgärderna. I särskilda fall får den tillsynsmyndighet (Datainspektionen) som är ansvarig för tillsyn av PuL besluta om vilka säkerhetsåtgärder som den personuppgiftsansvarige ska vidta (SFS 1998:204, 1998).

Personer som arbetar för den personuppgiftsansvariga får bara behandla personuppgifter enligt den personuppgiftsansvariges anvisningar. Om ett personuppgiftsbiträde används ska det finnas ett skriftligt avtal mellan biträdet och den ansvariga där det står att biträdet endast får behandla uppgifterna enligt instruktioner (SFS 1998:204, 1998).

2.1.7 Överföring till tredje land

Den personuppgiftsansvariga får enligt PuL inte överföra personuppgifter till ett land som inte upprätthåller lämplig säkerhet för personuppgifterna, vilket inkluderar lagring och behandling av uppgifterna (Cate, 1995; SFS 1998:204, 1998).

Det finns dock undantag från förbudet om den registrerade lämnar sitt samtycke till det eller om det är nödvändigt för att uppfylla avtal, rättsliga anspråk eller om den registrerades väsentliga intressen ska kunna tillgodoses. Det är även tillåtet om staten är ansluten till Europarådets konvention om automatisk behandling av individers personuppgifter (SFS 1998:204, 1998).

2.1.8 Sanktioner i PuL

Om en person bryter mot de bestämmelser som finns i PuL kan den personen straffas. Straffet som kan utdömas är böter eller fängelse i högst två år beroende på brottets dignitet. För att straffas vid brott mot PuL måste det som skett vara med uppsåt eller av hög oaktsamhet. Det kan inträffa att viss behandling av personuppgifter även är straffbart enligt andra lagar (Datainspektionen, 2018b).

Enligt PuL är det straffbart att inte lämna korrekta uppgifter till den registrerade eller till Datainspektionen, att strunta i att anmäla behandling av personuppgifter till Datainspektionen om sådan anmälan ska göras och att känsliga personuppgifter eller lagöverträdelseuppgifter behandlas på ett sätt som strider mot PuL. Det är även straffbart att känsliga personuppgifter eller lagöverträdelseuppgifter behandlas på ett kränkande sätt i material som är ostrukturerat och att i strid med de bestämmelser som finns i PuL överföra personuppgifter till tredje land utanför EU och EES (Datainspektionen, 2018b).

2.2 GDPR

GDPR kommer innebära en rad förändringar och skärpningar av PuL. En av de förändringarna som kommer ske är att missbruksregeln försvinner vilket innebär att oavsett om personuppgifterna är i strukturerat eller ostrukturerat material kommer GDPR att appliceras på dessa. Det innebär att om en organisation skickar e-post innehållande personuppgifter kommer det att beröras av GDPR (Ryz & Grest, 2016). Att missbruksregeln försvinner leder även till att uppgifter som tidigare inte varit berörda av PuL nu kommer att beröras av de nya kraven i GDPR (Brink, Elvland, & Hansson, 2017). Om en organisation har fler än 250 personer sysselsatta eller om behandlingen som organisationen genomför innebär särskilt stora risker ska det finnas ett register över vilken behandling som sker, vilket står i artikel 30 i Dataskyddsförordningen. Det är den personuppgiftsansvarige och/eller dess personuppgiftsbiträden som har ansvaret att ett sådant register upprättas. Registret ska t.ex. innehålla uppgifter om den personuppgiftsansvarige, i vilket syfte behandlingen sker, vilka kategorier av uppgifter som behandlas, vilka kategorier av tredje parter som uppgifter lämnas ut till och om möjligt beskrivning av tillämpade säkerhetsåtgärder (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016).

Det gäller alltså för organisationer att ha koll på hur och vilka uppgifter som de behandlar (Karlström, 2017).

Krystlik (2017) skriver att teoretiskt sett spelar det ingen som helst roll var data fysiskt lagras, GDPR kommer ändå att gälla för alla organisationer och företag som hanterar personuppgifter om europeiska medborgare. Definitionen av behandling i GDPR är nästintill likadan som i direktivet 95/46/EC och därmed även i PuL, vilket omfattar insamling, inspelning, strukturering, lagring, användning, radering anpassning och förändring av personuppgifter (Ryz & Grest, 2016). Även definitionen av personuppgifter är sig lik i GDPR jämfört med dataskyddsdirektivet där det egentligen bara är mindre omformuleringar i definitionen samt att lokaliseringsuppgifter och onlineidentiteter inkluderas som exempel (Europaparlamentets och Rådets Direktiv 95/46/EG, 1995; Europaparlamentets och Rådets förordning (EU) 2016/679, 2016).

I GDPR tillämpas samma definition för personuppgiftsansvariga och personuppgiftsbiträden som i PuL (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016; Datainspektionen, 2018c).

2.2.1 Samtycke i GDPR

På samma sätt som i PuL, ska ett samtycke vara specifikt, fritt och otvetydigt även i dataskyddsförordningen (Ryz & Grest, 2016). I GDPR har ett ansvar lagts på den personuppgiftsansvarige att bevisa att samtycke har givits av den registrerade. Det är även den personuppgiftsansvariges uppgift att lägga ner ett rimligt arbete för att verifiera att samtycket givits på laglig grund. Den registrerade ska även ha möjlighet att dra tillbaka sitt samtycke när som helst (Mittal, 2017).

Lotsson och Dobos (2016) skriver i en artikel att det inte längre kommer vara möjligt för företag att samla in samtycke genom svårlästa användaravtal eftersom att samtycket ska lämnas klart och tydligt. Om den registrerade drar tillbaka sitt samtycke måste all behandling av uppgifterna att upphöra, om det inte finns annan laglig grund för behandlingen, vilket i praktiken innebär att uppgifterna måste raderas ur organisationens system.

2.2.2 Information till den registrerade

När den registrerade ska lämna uppgifter till en personuppgiftsansvarig ska denne få information om personuppgiftsansvariges identitet och kontaktuppgifter, i vilket ändamål uppgifterna samlas in och varför de har att behandla uppgifterna, samt vilka som kommer att få ta del av uppgifterna, t.ex. tredje parter, vilket är liknande den information som ska ges enligt PuL. Utöver den informationen ska den registrerade få information om tidsperioder för behandlingen, vilka rättigheter den registrerade har gällande rätten till rättelse, radering, dataportabilitet, rätten till klagomål till tillsynsmyndighet och hur automatiserade beslut används samt grunderna i logiken som ligger bakom beslut. De ska även informeras hur vida den registrerade kan dra tillbaka sitt samtycke eller ej (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016).

För att ge den registrerade större rätt till sin egna data har denne rätt att få ut sina uppgifter i ett välkänt och maskinläsligt format, om personuppgifterna hanteras automatiserat och grundar sig på samtycke. Det kallas för rätten till dataportabilitet. Detta för att kunna överföra uppgifterna till en annan personuppgiftsansvarig. Det innebär att personens data blir portabel och kan flyttas från en personuppgiftsansvarigs organisation till en annan personuppgiftsansvarigs organisation (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016).

2.2.3 Rätten att bli bortglömd

Ett skärpt krav i GDPR är rätten för den registrerade att bli bortglömd, vilket innebär att när en person inte längre vill att en organisation ska behandla dennes uppgifter och det saknas annan laglig grund till behandlingen kan denne begära att bli borttagen ur deras system. Det är en rättighet som ska hjälpa personer att hantera sina dataskyddsrisker på ett bättre sätt (Ryz & Grest, 2016).

2.2.4 Säkerhet i GDPR

I GDPR, artikel 32, specificerades det att en lämplig säkerhetsnivå ska implementeras med hänsyn till den risk som finns med behandlingen och de merkostnader som uppstår vid införandet. Det för att säkerställa konfidentialitet, integritet och tillgänglighet vid behandlingen av uppgifterna (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016).

Två säkerhetsåtgärder som nämns är kryptering och pseudonymisering av uppgifter vilket innebär att man gör uppgifterna oläsbara för utomstående eller att man ser till att uppgifterna inte kan hänvisas till en specifik person utan ytterligare uppgifter som förvaras frånskilt från de pseudonymiserade uppgifterna (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016; Hert, 2016). Utöver kryptering och pseudonymisering nämner artikel 32 i dataskyddsförordningen även att lämpliga åtgärder ska vidtas för att inom en rimlig tid ha möjlighet att återställa tillgängligheten av data vid en teknisk eller fysisk incident.

För att upprätthålla den lämpliga säkerhet som krävs enligt GDPR bör organisationer ha en rutin för att regelbundet testa hur effektiva de implementerade åtgärderna är, vilket även det nämns i artikel 32 (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016).

Att tänka på säkerheten vid behandling och beslutande om hur behandlingen genomförs är viktigt i och med den nya reformen vilket beskrivs i Europaparlamentets och rådets förordning (EU) 2016/679 (2016) i artikel 25. Där står det att lämliga tekniska och organisatoriska åtgärder ska vidtas. Det för att organisationen ska ha möjlighet att skydda den registrerades rättigheter. I samma artikel skrivs det även lämpliga åtgärder ska vidtas för att som standard inte behandla fler uppgifter än vad som är nödvändigt i varje fall och uppgifterna ska bara behandlas under den tid som krävs för att uppfylla de intressen som finns. Den personuppgiftsansvarige ska ha kontroll så att personuppgifterna, som standard, inte offentliggörs till fler än vad som behövs. Det som beskrivs i artikel 25 kallas för inbyggt dataskydd och dataskydd som standard. Att arbeta med inbyggt dataskydd och dataskydd som standard innebär att integritetskyddande principer ska vitas redan i början när en personuppgiftsbehandling planeras.

2.2.5 Överföring till tredje land

Ryz och Grest (2016) skriver att *Article 29 working party*, som är en oberoende arbetsgrupp som etablerades under dataskyddsdirektivet och fungerar som rådgivare för dataskydds- och integritetsfrågor, skriver i WP158 att all filtrering av personuppgifter ska ske lokalt i landet där uppgifterna samlats in och innan de skickas till ett annat land. *Article 29 working partys* råd är inte bindande men är inflytelserika.

2015 dömde den europeiska domstolen att *Safe Harbour*-överenskommelsen inte längre var giltig och därmed har inte organisationer baserade i USA laglig rätt att överföra information om EU-medborgare från EU till USA. Detta eftersom att *Safe Harbour*-avtalet inte skyddar integriteten tillräckligt väl då det är 15 år gammalt och inte möter den teknologiska förändring som skett (Ryz & Grest, 2016; Krystlik, 2017). Ryz och Grest skriver vidare att det finns ett nytt avtal, som uppfyller samma princip som *safe Harbour*, och benämns som *EU-US privacy shield* där ett av kraven är att USA ska ha en ombudsman som hanterar klagomål från europeiska medborgare om att USA spionerar på data om dem.

2.2.6 Krav att anmäla intrång

Om ett intrång sker mot organisationen där det finns risk att personuppgifter har kommit på villovägar har organisationer skyldighet att dokumentera och anmäla intrånget till den myndighet som ansvarar för de uppgifterna, Datainspektionen i Sverige, inom 72 timmar efter att de blivit medvetna om att intrånget skett (Ryz & Grest, 2016; Datainspektionen, 2017a). Det benämns ibland som incidentrapportering.

Om den inträffade incidenten kan ha stor individuell påverkan ska de berörda individerna informeras direkt om incidenten.

2.2.7 Sanktioner enligt GDPR

Sanktioner vid brott mot GDPR kommer innebära att organisationer riskerar böter på upp till mellan 2–4% av den globala omsättningen eller 10–20 miljoner euro beroende på vilka delar av GDPR som inte uppfylls. Saker som påverkar sanktionsavgiftens storlek kan även variera beroende på t.ex. vilken karaktär det bristande införandet har, vilken typ av personuppgifter som berörs, om det har skett med uppsåt eller inte, etc. (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016; Ryz & Grest, 2016).

2.3 Tekniska lösningar för uppfyllandet av dataskyddslagstiftning

I och med att lagar ska gälla under en lång tid och att de kan vara svåra att förändra brukar lagar och bestämmelser inte nämna några särskilda tekniska lösningar för att uppfylla det som står i lagtexten. Det finns dock ett undantag och det är i GDPR där det explicit skrivs om kryptering. Om en organisation har implementerat kryptering på ett korrekt sätt, dvs. genom att ha en beprövad krypteringsalgoritm och att krypteringsnycklarna hålls oåtkomliga för utomstående, är de inte skyldiga att informera den registrerade vid intrång (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016; Krystlik, 2017; Tankard, 2016).

Tankard (2016) skriver att kryptering är den ledande teknologin för att kontrollera dataskydd samt att den primära drivkraften för att använda kryptering är att skydda mot incidenter kring dataläckage. Eftersom att kryptering explicit står utskrivet i GDPR innebär det att kryptering är standardvalet gällande skydd av personuppgifter både vid överföring och lagring. Om data lagras i molntjänster är det organisationens skyldighet att se till att krypteringsnycklarna förvaras säkert så ingen tredje part kan komma åt den data som finns sparad. Även om kryptering är en bra teknik för att skydda data kommer det inte att räcka med enbart det. För organisationer kommer det vara viktigt att ha en bra och beprövad åtkomstkontroll för att se till att obehöriga inte får åtkomst till data när den är avkrypterad, för att lösa en sådan åtkomstkontroll kan t.ex. en katalogtjänst användas (Datainspektionen, 2008; Tankard, 2016).

Som tidigare nämnts har den registrerade rätt till radering i vissa fall då det inte föreligger någon annan bestämmelse som kräver fortsatt behandling. För att den registrerade ska kunna begära det måste organisationer ha koll på vilken information de behandlar om de registrerade vilket Brink et al. (2017) skriver om i sin rapport. De beskriver även problemet med rätten till radering i säkerhetskopior som organisationer underförstått måste ha för att uppfylla möjligheten att återfå tillgänglighet till data inom rimlig tid vid en incident. Det kan vara en omöjlig sak att lösa i enlighet med GDPR. Det eftersom att vid radering kan backuperna innehålla för mycket data för att de ska vara möjligt att söka igenom för radering. Ett annat alternativ för raderingen kan vara att föra ett register över vilken data som ska bli borttagen om en backup måste återställas vilket de beskriver kan vara brott mot dataskyddsförordningens bestämmelser.

Brink et al. (2017) skriver att leverantören av systemen har som uppgift att se till att systemen uppfyller de krav som finns i dataskyddsförordningen när det kommer till integritet, tillgänglighet och konfidentialitet. Det är sedan upp till den användande verksamheten att regelbundet testa systemen för att säkerställa att säkerheten fungerar och är tillräcklig med beaktande av de uppgifter som behandlas. Det är även något som Bitar och Jakobsson (2017), Datainspektionen (2008) och Tankard (2016) skriver om. Organisationer behöver alltså rutiner och/eller system för att övervaka att säkerheten fungerar, dels för att uppfylla de bestämmelserna om regelbunden testning men även för att kunna informera om personuppgiftsincidenter.

Ett sätt att kommunicera internt i en organisation är via e-post. Under PuL kan organisationer använda e-post som kommunikationssätt när de kommunicerar om personuppgifter såvida det inte kränker den registrerade, och att det inte gör något om någon skulle läsa det, eftersom att det räknas som ostrukturerat material, som är undantaget från PuL (Datainspektionen, 2018e). Men eftersom att missbruksregeln försvinner i och med införandet av GDPR, måste organisationer genomföra samma bedömning för personuppgifter som behandlas i e-post som för andra personuppgifter. Detta för att upprätthålla en lämplig säkerhetsnivå samt ha en legal grund för behandlingen. Enligt Datainspektionen (2018a) kan en organisation som regel alltid hantera inkommande e-post med stöd av allmänt intresse. Det som dock kan bli ett bekymmer är hur länge det får lagras som e-post, vilket kan lösas genom att flytta de viktiga uppgifterna till ett annat system. Både under PuL och GDPR bör organisationer undvika att skicka känsliga personuppgifter via e-post, speciellt om den inte är krypterad, eftersom att meddelandena kan

komma att skickas över öppna nätverk, och därmed kan potentiellt vem som helst läsa det (Datainspektionen, 2018e; Datainspektionen, 2018a).

För att uppfylla rätten till dataportabilitet bör organisationer vara medvetna om vilken typ av uppgifter som de behandlar som grundar sig på samtycke. Den tekniska lösning som sedan krävs är att organisationens system har möjlighet att exportera uppgifterna till ett välkänt och maskinläsligt format (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016). Den personuppgiftsansvarige bör se till att den registrerade har möjlighet att själv få ut sina uppgifter för eget bruk. Det kan förslagsvis ske genom att tillhandahålla den registrerade en möjlighet att ladda ner uppgifterna och sekundärt se till att den registrerade kan överföra uppgifterna till en annan personuppgiftsansvarig (Article 29 data protection working party, 2018). Enligt Article 29 data protection working partys riktlinjer om rätten till dataportabilitet (2017) bör varje fall genomgå en bedömning om det är tekniskt möjligt för en personuppgiftsansvarig att överföra uppgifter till en annan, eftersom att en personuppgiftsansvariga inte är skyldiga att ha system som kompatibla med varandra på ett tekniskt plan. Article 29 working party (2017) skriver att syftet med dataportabiliten är att systemen inte ska vara helt kompatibla med varandra utan att de ska vara driftskompatibla system. Vilket format som sedan är lämpligast att använda beror på i vilken bransch som organisationen verkar inom och vad som är vanligt där, det står dock fast att det förväntas att ett format där det är lätt att extrahera uppgifter och sortera ut det som är lämpligt bör användas. Skulle det inte finnas något välanvänt format inom den givna branschen bör uppgifterna kunna tillhandahållas i andra öppna format såsom CSV, JSON eller XML (Article 29 data protection working party, 2017).

2.4 Tidigare arbeten

Det finns många tidigare arbeten som berör PuL, GDPR och de förändringar som kommer beröra av organisationer. De arbetena går igenom delar av de båda lagstiftningarna och kommer fram till att stora delar kommer vara densamma efter införandet av GDPR, men att även kommer till nya och striktare krav på verksamheterna (Brink et al., 2017; Mittal, 2017; Ryz & Grest, 2016). Att veta likheter och skillnader på bestämmelserna är en viktig del av den här undersökningen för att veta vad företag kan tänkas behöva förändra i sina system för att uppfylla de nya kraven.

En sak som det inte finns så många tidigare arbeten om är vilka tekniska förändringar som kan beröras av införandet av GDPR, men det är något som Tankard (2016) går igenom i sin artikel, *What the GDPR means for businesses*. Tankard nämner olika tekniska lösningar, t.ex. kryptering och åtkomstkontroller, som är relevanta för att skydda personuppgifter och därmed uppfylla delar av GDPR. Men trots att Tankard tar upp en del av de tekniska aspekter som GDPR innebär finns det dock luckor kvar att undersöka. Det är exempelvis vad organisationer har för lösningar idag och vad de för in för tekniska lösningar i sin verksamhet under anpassningen till GDPR.

Karlström (2017) har gjort ett arbete där han tar fram ett ramverk för att organisationer ska kunna kontrollera hur förberedda de är inför GDPRs införande. Ramverket har han tagit fram genom att genomföra en litteraturstudie samt att intervjua personer som har en god insyn i

arbetet med GDPR för att då kunna identifiera förberedelseaktiviteter som bör genomföras. Ramverket har sedan testats mot ett antal företag från inkubatorer och teknikparker i Sverige. I ramverket finns det bland annat en del som behandlar tekniska åtgärder som kan komma att användas i den här undersökningen. Förberedelser som kan vidtas inkluderar t.ex. kryptering av personuppgifter, processer för att ha uppdaterade mjukvaror och system, loggning och övervakning av personuppgifter samt begränsning för vem som har tillgång till de olika uppgifterna, vilket kan vara förändringar som företag kan tänkas behöva göra på ett tekniskt plan för att förbereda sig inför GDPR.

3 Problemformulering

I det här kapitlet diskuteras syftet med arbetet och den forskningsfråga som arbetet ska bygga på för att uppfylla arbetets syfte. Forskningsfrågan motiveras även baserat på andra källor som finns inom området. Avgränsningar motiveras i form av organisationsval.

3.1 Problembakgrund

I och med digitaliseringen av samhället och att allt fler och fler personuppgifter behandlas av organisationer dagligen ligger införandet av GDPR i tiden. Att organisationer behandlar personuppgifter i sin verksamhet är något som är en självklarhet, både för organisationen och för individen själv som dagligen delar med sig av personuppgifter (Ryz & Grest, 2016) på internet och till organisationers medlemskap. Meglena Kuneva, som var konsumentkommissionär i EU, jämförde personuppgifter med olja under ett tal 2009 för att visa hur information har blivit en viktig del av ekonomin (Kuneva, 2009; Spiekermann, Acquisti, Böhme, & Hui, 2015). Verksamheterna och företagen använder sig av informationen för att göra analyser med syfte att utveckla sin verksamhet och på så sätt skapa ett mervärde för konsumenterna (Spiekermann et al. 2015). På grund av att informationen är en sådan viktig del för företagen tillkommer givetvis nackdelar med att behandla så pass mycket information som många företag gör. Spiekermann et al. (2015) skriver att informationsbehandlingen kan bli en påfrestning, dels för att olika länder har olika dataskyddslagar och dels risken att bli utsatt för IT-brott i form av intrång. För att undvika intrång så långt det går måste företag ständigt jobba med tekniska och organisatoriska processer för att anpassa sig.

För att individen ska känna sig trygg och få ett större inflytande av sina personuppgifter som organisationer behandlar och för att EU ska ha en gemensam dataskyddslagstiftning införs GDPR (Lotsson & Dobos, 2016; Mittal, 2017). Eftersom organisationer har haft ett stort flöde av olika typer av uppgifter behöver de se över sina verksamheter för att anpassa sig till den nya lagstiftningen. Arbetet med kartläggningen av uppgifter och hanteringen av dessa är ett stort jobb som även kan anses vara tidskrävande. I och med anpassningen kommer flera delar av verksamheterna att beröras, det gäller allt ifrån deras tekniska system som de använder dagligen till hur de dagligen arbetar med att behandla personuppgifter. Att skydda sig mot felaktig behandling av uppgifter går inte enbart ut på att ha säkrade system som ingen utomstående kommer åt, utan det innefattar även olika processer och rutiner för hur behandlingen ska gå till, t.ex. hur personuppgifter ska kommuniceras mellan medarbetare. Men för att de processerna

och rutinerna ska fungera krävs det att verksamheten har tekniska system som fungerar och är anpassade till det nya beteendet.

Det finns många tidigare arbeten som tar upp jämförelser mellan PuL och GDPR, det finns även arbeten och artiklar om vad organisationer behöver göra för att förbereda sig. Men i och med att flera säkerhetsåtgärder nämns explicit i GDRP (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016) och att det införs hårdare krav på hur organisationerna får behandla uppgifter indikerar det på att företag kan behöva införa nya tekniska lösningar. Syftet med det här arbetet är att försöka ta reda på vilka tekniska lösningar företag redan hade implementerade i sin organisation under PuL och vilka nya tekniska lösningar som behövs för att uppfylla de nya och hårdare kraven. GDPR träder snart i kraft och då ska organisationer redan ha implementerat eller ha en plan för införandet av GDPR för att undvika höga sanktionsavgifter.

3.2 Motivering

Poullet (2006) skriver att organisationer inte har prioriterat att uppfylla de krav som ställs i dataskyddsdirektivet, dels för att de fått ett litet antal klagomål och dels för att det är låg detekteringsrisk vid ej uppfyllda krav. Det gäller även svenska PuL som inte införts korrekt, vilket Svanfeldt (2006) skriver om.

Svanfeldt skriver vidare att det i Sverige är ovanligt att brott mot PuL leder till åtal och om de gör det är det bara några få personuppgiftsansvariga som döms till dagsböter. Sveriges radio (2013) skriver att det är tre av 200 fall om brott mot PuL som lett till åtal mellan åren 2007–2013.

Som tidigare nämnts träder snart GDPR i kraft och då är det inte enbart PuL som ska uppfyllas utan det är delvis nya och striktare krav. Om organisationer redan har implementerat PuL bör arbetet med att införa GDPR minska drastiskt då det finns likheter mellan de båda personuppgiftsskyddande lagstiftningarna. Men trots att delar redan är lag kan nya tekniska system behöva införas eftersom att det hela tiden kommer nya tekniska lösningar för att behandla uppgifter på säkrare sätt. Att företag och organisationer nu har uppmärksammat att de måste uppfylla de nya kraven i GDPR kan kanske beskrivas genom att alla verksamheter har personuppgifter lagrade i någon form i olika typer av databaser, vilket Krystlik (2017) skriver i en artikel, och genom de höga sanktionsavgifterna som kan utdömas vid ett misslyckande av införandet och uppfyllandet av GDPR (Krystlik, 2017).

Brink et al. (2017) har gjort ett arbete där de jämför PuL och GDPR där de kommer fram till att ett intressant fortsatt arbete skulle vara att genomföra en undersökning av implementeringen av GDPR precis innan den träder i kraft. Men eftersom att GDPR inte trätt i kraft ännu kan inga krav ställas på att organisationer ska vara helt färdiga med implementationen och därför bör huvudfokus ligga på likheterna mellan PuL och GDPR, men även inkludera hur organisationer har planerat att hantera delar av de nya bestämmelserna i GDPR.

3.3 Forskningsfråga

Den forskningsfråga som ska besvaras i undersökningen för att syftet med undersökningen ska uppnås är:

Vad har företag med möjlighet att kartlägga konsumtionsvanor infört för nya tekniska lösningar för att uppfylla den nya dataskyddslagstiftningen (GDPR) i jämförelse med kraven i PuL?

För att besvara frågeställningen kan forskningsfrågan delas upp i två delfrågor:

1. *Vilka tekniska lösningar har ni som organisation vidtagit för att uppfylla PuL?*
2. *Vad har ni behövt förändra till införandet av GDPR?*

3.4 Val av organisationer

Nästintill alla organisationer behandlar personuppgifter på ett eller annat sätt i sin dagliga verksamhet och därför bör vilken organisation som helst kunna vara föremål för undersökningen. Men eftersom att bestämmelser i andra lagar har högre dignitet, vid motsägelser i lagarna, i förhållande till PuL och kommande GDPR kan det vara intressant att fokusera på sådana organisationer som inte behandlar personuppgifter baserat på andra lagar än PuL och GDPR. Det bör i så fall finnas någon form av samtycke till behandlingen av personuppgifter.

Ett exempel på personuppgifter som behandlas är shoppingvanor, som användare dagligen delar med sig av vilket EU-kommisionären Jourová (2018), med ansvar för rättsliga-, jämställdhets-, och konsumentfrågor skriver om. Köpvanor kan t.ex. samlas in genom att du som kund samtycker till det genom ett avtal vid registrering av medlemskapet till exempel en kundklubb eller registrering på en webbutik. Den gemensamma nämnaren i urvalet av organisationer är alltså att de har möjlighet att genom samtycke samla in köpvanor om den registrerade.

I både PuL och GDPR finns det bestämmelser om att den registrerade har rätt att invända mot behandling som är avsedd för direkt marknadsföring (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016; SFS 1998:204, 1998). Undersökningen avgränsas därför till företag som har möjlighet att kartlägga konsumtionsvanor.

3.5 Förväntat resultat

Baserat på Poullet (2006), Svanfeldt (2006) och Sveriges radio (2013) bör det förväntade resultatet vara att organisationer inte har de tekniska lösningar som krävs för att uppfylla PuL och än mindre de nya bestämmelserna i GDPR. Men eftersom att GDPR träder i kraft den 25 maj 2018 bör organisationer ha genomfört en rad olika tekniska förändringar för att uppfylla GDPR, speciellt om de inte har tagit PuL på så stort allvar och haft de lösningar som krävs. Målet med undersökningen är att ta reda på vilka tekniska lösningar som redan finns på plats och som de planerar att införa.

4 Metod

I följande kapitel beskrivs det att en intervjustudie är tänkt att användas för att genomföra undersökningen. Valet av metod motiveras även med hänsyn till undersökningens syfte. Efter att metodvalet diskuterats kommer även ett intervjuunderlag tas fram och presenteras baserat på den tidigare presenterade bakgrunden och forskningsfrågan. Därefter behandlas etiska aspekter och validitetshot.

4.1 Intervjustudie

Att använda sig av en kvalitativ metod lämpar sig ofta bra om man vill försöka få en djupare förståelse inom området framför att få en förklaring kring det och kan användas för att undersöka organisatoriska aspekter i förhållande till teknik (Berndtsson, Hansson, Olsson, & Lundell, 2008). Eftersom att anpassningen till GDPR antagligen ser ut på helt olika sätt i alla organisationer lämpar sig en kvalitativ studie bra eftersom den utgår från att verkligheten kan uppfattas på olika sätt beroende på vem man partar med och det kan därför vara svårt att forma och precisera enkätfrågor för att få svar på forskningsfrågan (Hedin, 1996). Berndtsson et al. (2008) skriver även att intervjuer kan användas inom kvalitativa undersökningar och menar på att det finns två former av intervjustudier, vilka är strukturerade och ostrukturerade intervjuer. En strukturerad intervju bygger på att intervjuaren har ett bestämt antal frågor som ska ställas vilket inte lämnar något utrymme för att lägga till eller ta bort frågor baserat på respondentens svar. Den typen av intervjuer har som fördel att det är lätt att replikera intervjun oavsett vem som intervjuar. De ostrukturerade intervjuerna bygger på att inte ha förberett några specifika frågor utan intervjun bygger på dess syfte. Därför kan det kräva en del erfarenhet av intervjuaren för att vara kapabel till att ställa öppna frågor, som kan besvaras med respondentens egna ord, och samtidigt uppnå intervjuns syfte. Det är lätt att sväva iväg och då inte uppnå intervjuns syfte, vilket även gör det svårt att replikera intervjun och därmed studien.

För att genomföra en kvalitativ undersökning på hur organisationer arbetar kring tekniska lösningar inom PuL och GDPR anses en intervjustudie vara bra därför att det enligt Edwards & Holland (2013) är en vanlig typ av undersökning för att få kvalitativa svar. Edwards & Holland (2013) beskriver även de två formerna av intervjuer och lägger även till en ny form, semi-strukturerad, som är en blandning av de två tidigare nämnda. För att intervjuerna ska bli valida och uppnå sitt syfte anses semi-strukturerade intervjuer vara bra för att inte sväva iväg för mycket under själva intervjun. Den semi-strukturerade intervjun kommer att bygga på ett visst antal fördefinierade, öppna frågor, som respondenten själv kan utveckla svaret på. Bedömningen är att det är viktigare att få kvalitativa svar baserat på det fördefinierade frågeunderlaget, som är utformade efter forskningsfrågan, framför att ställa exakt samma följdfrågor till alla respondenter.

4.2 Analys av intervjuer

För att analysera intervjuerna kommer en innehållsanalys att användas, vilket är en vanlig typ av analys när det kommer till kvalitativa undersökningar (Hsieh & Shannon, 2005). Innehållsanalys går ut på att intervjun analyseras både som helhet och som utplockade textavsnitt och fraser som är viktigt för frågeställningen (Eklund, 2012; Graneheim &

Lundman, 2004). Enligt Eklund (2012) är det bra om analys av en intervju påbörjas så snart det är möjligt efter att den är genomförd istället för att vänta tills alla intervjuer är genomförda. Graneheim & Lundman (2004) menar även att analysen är en iterativ process, vilket innebär att analysen utförs flera gånger genom att varva helhetsanalys av texten och delar av texten för att få med alla de viktiga aspekterna som går att få av intervjuerna. Under analysen kommer intervjuerna att läsas igenom flera gånger för att få en bred förståelse för vad som sägs. Under tiden de läses igenom kommer relevanta textavsnitt att tas ut för att dela in de under två huvudkategorier, vad företag gjort för att uppfylla PuL och vad de har gjort för förändringar. De två huvudkategorierna har sedan flera underkategorier som bygger på de olika intervjufrågorna, t.ex. säkerhetsåtgärder, rätten till rättelse, rätten till radering, missbruksregelns försvinnande, dataportabilitet, osv. De mest relevanta textavsnitten presenteras sedan sammanfattande under resultatet tillsammans med en analys vars syfte är att jämföra och återkoppla mot den tidigare presenterade teorin.

4.3 Underlag till intervjufrågor

För att formulera intervjufrågor har forskningsfrågorna använts eftersom att de ska besvaras och är baserade på bakgrunden och undersökningens syfte. Intervjufrågorna kan kategoriseras in under tre delar, en del med allmänna frågor, en del som fokuserar på tekniska lösningar för att uppfylla PuL (delfråga ett) och en som fokuserar på vilka förändringar de behövt vidta för GDPR (delfråga två). Intervjufrågorna finns i sin helhet i Bilaga A.

4.4 Genomförande av intervjuer

Som tidigare beskrivits så baserar sig urvalet på företag som har försäljning av någon typ av produkter samt att de ska ha möjlighet att kartlägga kundens konsumtionsvanor. Kartläggningen kan ske antingen via ett medlemskap i form av en kundklubb eller genom att kunden registrerar sig på deras webbutik. För att få tag på företag som vill ställa upp på en intervju har lämpliga kandidater kontaktats, vilket oftast skedde via telefon men även per e-post i vissa fall då telefonnummer inte gick att hitta, eller att de kontaktade företagen velat ha förfrågan per e-post. För att hitta kandidater att kontakta har Google-sökningar använts för att hitta antingen företag som har butiker med kundklubb eller haft en webbutik med möjlighet till registrering av konto. Vid kontakt med kandidaterna har undersökningens syfte beskrivits för att sedan fråga om de har tid och möjlighet att ställa upp på en intervju. Eftersom att det är en kvalitativ intervjustudie som genomförs bedöms det att endast ett fåtal respondenter behövs. I det här fallet är bedömningen att minst fem stycken respondenter (Hedin, 1996), och därmed fem olika företag, behövs för att ha möjlighet att genomföra en analys av insamlade data och därmed kunna svara på forskningsfrågan.

När ett företag väl har sagt ja till att ställa upp på en intervju har intervjuunderlag skickats till de för att ge de möjligheten att förbereda sig och ta reda på saker som de inte känner till då arbetet med PuL och GDPR kan vara omfattande vilket även bör leda till att intervjun får mer relevant data att analysera. Intervjuerna kommer även att spelas in, vilket respondenterna får information om samt möjlighet att samtycka till det, och transkriberas för att underlätta analys av insamlade data. Under själva intervjun används intervjuunderlaget som redan beskrivits som stöd för den semi-strukturerade intervjun, vilket innebär att i stora drag har intervjun tre delar.

En del om allmänna frågor om respondenten och allmänt om personuppgifter, en del om hur de hanterade tekniska lösningar i PuL samt den avslutande del om hur den har tänkt att hantera GDPR.

4.5 Analys av samtyckessavtal

För att organisationerna ska ha möjlighet att lagra och behandla köpvanor måste de ha legal rätt till att behandla den typen av personuppgifter. Detta sker ofta genom att den registrerade ger sitt samtycke till behandlingen genom ett avtal. De avtal som analyseras tillhör de organisationer som har intervjuats och benämns på deras hemsidor som integritetspolicy, medlemsvillkor, eller andra dokument där de beskriver hur deras behandling genomförs. Bedömningen att analysera avtal för insamlandet av samtycke till sådan behandling av uppgifter kan ge undersökningen en ytterligare trovärdighet samtidigt som det minimerar undersöknings risk, eftersom att flera datainsamlingsmetoder används. Undersökningen förlitar sig därmed inte enbart på att intervjuerna ska ge tillräckligt med data för att uppnå undersökningens syfte.

Den analys som kommer att genomföras på samtyckesavtalen, där den registrerade samtycker till behandling av personuppgifter, kommer gå ut på att kontrollera om de beskriver hur behandlingen kommer att gå till. För att analysen ska genomföras på ett strukturerat sätt har följande frågor tagits fram för analysen.

- Vad skriver de om tekniska lösningar i behandlingen?
- Vilken typ av information lämnas till den registrerade innan samtycke ges?
- Nämns några av den registrerades rättigheter som finns i PUL? T.ex. rätten att få ut information, rättelse av felaktiga uppgifter, hanteringen av uppgifter i marknadsföringssyfte.
- Nämns några av de nya koncepten som införs i och med GDPR? T.ex. rätten att bli bortglömd, rätten till dataportabilitet.

Om ett avtal enbart nämner koncept som finns i PuL och ingenting om de nya kraven som t.ex. rätten att bli bortglömd och rätten till databortabilitet, går det kanske att anta att de i skrivande stund inte är helt och hållet förberedda inför GDPR.

Det är viktigt att analysen knyter an till undersökningens syfte och de tidigare beskrivna teorierna (Skrivguiden, 2018) om PuL och GDPR vilket den gör vid användandet av de ovanstående punkterna.

4.6 Etiska aspekter

Vetenskapsrådet (2002) beskriver fyra krav som bör beaktas vid undersökningar. De fyra kraven är informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Informationskravet bygger på att informera intervjuobjektet om vad de har för uppgift i undersökningen. Även vad de har för villkor inklusive att deltagandet är av frivilja och att de kan avbryta sitt deltagande när de vill. I informationskravet ska även syftet och tillvägagångssätt presenteras. Samtyckeskravet innebär att samtycke till deltagande ska inhämtas från intervjuobjektet. Konfidentialitetskravet säger att de deltagande personerna ska

ges konfidentialitet och att uppgifter som kan identifiera enskilda personer, och i den här undersökningen eventuellt även organisationer, bör hållas hemliga och oåtkomliga för utomstående, och alltså inte publiceras. Det sista kravet, nyttjandekravet, säger att de insamlade uppgifterna endast får behandlas inom ramen för undersökningen.

Undersökningen kan komma att hantera data som organisationer kan anse vara känslig att dela med sig av, dvs. mer ingående hur de behandlar personuppgifter. En organisation som inte kommer hinna slutföra arbetet med GDPR kommer kanske inte vilja gå ut med sådan information offentligt, med hänsyn till sanktionsavgifterna. Därför kommer anonymitet för organisationer och intervjupersoner tas på allvar genom att beakta konfidentialitetskravet (Vetenskapsrådet, 2002) som tidigare nämnts.

Även om de organisationer som ställer upp anser sig hinna med anpassningen till GDPR kan det vara så att de inte vill gå ut med hur de behandlar personuppgifter på grund av olika anledningar. Även dessa organisationer kommer hållas anonyma i undersökningen.

Att spela in intervjun anses vara viktigt för att ha möjlighet att genomföra en rättfärdig analys, vilket gör det möjligt att transkribera intervjun och därmed undvika att delar missuppfattas eller missas om anteckningar måste tas under själva intervjun. För att kunna hantera anonymiteten kan delar av intervjuerna komma att maskeras i transkriberingen för att undvika möjlighet till identifikation.

4.7 Validitetshot

För att de genomförda intervjuerna ska ha validitet och reliabilitet får intervjuobjekten möjlighet att läsa igenom transkriberingen av intervjun för att ha möjlighet att göra tillägg och ändringar på det som sagts. Det är viktigt att låta intervjuobjekten få den möjligheten enligt Berndtsson et al. (2008) för att kunna göra påståenden i analysen.

Wohlin et al. (2012) skriver om att validitetshot kan delas upp i olika kategorier. De kategorierna är slutsatsvaliditet (eng. *conclusion validity*), konstruktionsvaliditet (eng. *construct validity*), intern validitet (eng. *internal validity*) och extern validitet (eng. *external validity*).

Slutsatsvaliditet innehåller ett validitetshot som benämns som *Fishing and the error rate* och innebär att undersökaren aktivt letar efter ett speciellt svar i undersökningen vilket gör att analysen inte blir oberoende (Wohlin, et al., 2012). För att hantera det validitetshotet kommer intervjufrågorna att finnas med i bilagorna för att visa vad intervjuerna bygger på. Det här validitetshotet finns med under hela arbetets gång samtidigt som intervjuerna och dess analys kommer att hanteras på ett objektivt sätt.

Kategorin Extern validitet har ett validitetshot som benämns som *Interaction of selection and treatment* och kan innebära ett hot mot den här undersökningen. Det kan förklaras med att det är viktigt att rätt personer ställer upp som respondenter eftersom att undersökningen bygger på ett kunskapsområde som inte alla känner till (Wohlin, et al., 2012). För att hantera det gäller det att försöka vara noggrann i urvalet av intervjupersoner och hela tiden var tydlig med vad undersökningens syfte är och vilken kompentens respondenten behöver för att kunna ställa upp.

Inom kategorin konstruktionsvaliditet finns det en underkategori som benämns *Social threats to construct validity* och innebär att respondenterna i det här fallet kan agera och svara annorlunda när de vet om att de deltar i en undersökning (Wohlin, et al., 2012). För att hantera det hotet är det bra att så långt det är möjligt låta respondenten välja plats för intervjun så att denne känner sig trygg i den miljön.

Ett internt validitetshot är *Maturation* vilket innebär att respondenten kan ändra beteende med tiden, om denne t.ex. blir trött eller uttråkad. *Maturation* hanteras genom att skicka ut intervjuunderlaget till respondenterna innan intervjuerna för att de ska kunna förbereda sig och därmed kan intervjusessionerna fortskrida snabbare. Ett annat validitetshot inom kategorin intern validitet är *Instrumentation* vilket innebär att insamlingsinstrumenten, i det här fallet intervjufrågorna, är dåligt designade och kan därmed påverka undersökningen negativt (Wohlin, et al., 2012). För att hantera dåligt designade intervjufrågor kommer de att utgå från forskningsfrågan och de två delfrågorna som specificerats med beaktande till den bakgrund som presenterats.

5 Resultat

I det här kapitlet kommer en presentation av verksamheterna och respondenterna samt resultatet från intervjuerna och från medlemsavtalen att presenteras på ett objektivt och sammanfattande sätt. Resultatet kommer bygga på de två delfrågorna som tidigare presenterats, dvs. vad det gjort för att uppfylla PuL och vad de gjort för förändringar.

5.1 Presentation av organisationer

Här presenteras de organisationer som deltagit i undersökningen med vad de baserar sitt insamlande av personuppgifter på och vad de använder de till. Respondenten på varje organisation presenteras även för att skapa förståelse hur de är involverade i organisationens tekniska lösningar i förhållande till GDPR.

5.1.1 Organisation A

Organisation A har en kundklubb där de behandlar uppgifter som personnummer och namn. Respondenten är inte helt säker på hur de använder konsumentens köpvanor inom organisationen, men uppger att de troligtvis använder sig av de för att göra analyser på vad som köps men inte för konsumentspecifika erbjudanden. Respondenten själv har titeln IT-säkerhetschef och är involverad i huvuddelen av deras GDPR-projekt och är delprojektledare för ITs del.

5.1.2 Organisation B

Organisation B har företag som huvudkundgrupp, men de har även en butikskedja med en kundklubb där privatpersoner kan bli medlemmar. De använder sig av personuppgifterna i kundklubben för att göra analyser på en generell nivå då de inte enligt respondenten är intresserade av vad en specifik kund köper utan tittar på artikel-butik-område. Uppgifterna de behandlar är telefonnummer, adress och namn. Respondenten är involverad i GDPR-arbetet genom att denne är med i deras projektgrupp och har titeln IT-chef.

5.1.3 Organisation C

Organisation C har sin IT-drift hos en extern part, dvs. *outsourcad*. De behandlar personuppgifter i sin kundklubb, vilket kan vara namn, adress och köphistorik. Uppgifterna används sedan för att bygga en relation med kunderna och därmed öka trafiken till deras butiker genom att erbjuda kunden erbjudanden baserat på köp. Informanten uppger att denne är projektledare och därmed ansvarig för deras interna GDPR-projekt.

5.1.4 Organisation D

Organisation D behandlar uppgifter som personnummer, köphistorik, etc. i sin kundklubb. Uppgifterna använder de sedan för att kunna erbjuda konsumenter en konkurrenskraftig köpupplevelse genom att ge erbjudanden baserat på konsumtionsmönster. Informanten som deltagit är CIO/IT-chef för delar av koncernen och är ägare av deras GDPR-projekt.

5.1.5 Organisation E

Organisation E behandlar personuppgifter i deras kundklubb vilket är namn, personnummer, köpinformation och kontaktuppgifter. Uppgifterna använder de sedan för att analysera kundbeteenden för att ta reda på vem som köper vad och vilka deras målgrupper är. Uppgifterna som de behandlar kan i vissa fall klassas som lite känsligare då vissa varor kan avslöja en konsuments fysiska tillstånd. Informanten har varit involverad i deras GDPR arbete genom kartläggning av deras befintliga information samt hur de ska hantera den för att följa GDPR. Informantens titel är CIO/IT-chef.

5.2 Resultat från intervjuer

Resultatet från intervjuerna har tagits fram genom att läsa igenom transkriberingen av intervjuerna för att sedan föra in relevanta delar och meningar i en tabell. Tabellen baserar sig på de två delfrågorna som tagits fram ifrån forskningsfrågan, dvs. tekniska lösningar under PuL och förändringar inför GDPR. De två kategorierna har sedan underkategorier med huvudområden som tagits upp under intervjuerna och baserar sig då alltså på intervjuunderlaget och dess olika delar. I resultatet kommer relevanta textavsnitt från de olika informanterna att presenteras.

5.2.1 Vilka tekniska lösningar har ni som organisation vidtagit för att uppfylla PuL?

För att uppfylla den säkerhet som krävs i PuL, dvs. en lämplig säkerhetsnivå, har t.ex. organisation B valt att använda sig av krypterade anslutningar mellan deras IT-miljö och butikens kassor.

> *[…] hälften av butikerna sitt ju på vårat privata datanät så de finns ju inte någonstans och de butikerna där vi använder internet som access hit så har vi ju givetvis krypterad VPN-tunnel mellan oss och butiken.*
> – Organisation B

Organisation D däremot uppger att för att få ut uppgifter ur databasen så måste en nyckel användas, dvs. uppgifterna är troligtvis krypterade.

Den kopplas med nyckel, så att då när du slår i kunddatabasen måste du ha nyckeln med dig, och då kan du få ut uppgifterna så att säga.
– Organisation D

Under intervjuerna med organisation A och B framgick det att de har använt sig utav penetrationstester för att förbättra sin säkerhet. Informanten från organisation B kommenterar det på följande vis:

[…] så får man åtgärdsschema, det var inget roligt schema första gången kan jag säga. Men så var det, det var bara sätta igång och patcha.
– Organisation B

I övrigt när det gäller säkerhetslösningar för att säkra de uppgifter som behandlas uppger organisation A att de har jobbat en del med åtkomstbegränsningar.

Vi har haft en del interna rutiner för att hantera det här, men det är ju behörighets delarna då, där vi liksom har en viss styrning över åtkomsten av personuppgift då
– Organisation A

Alla organisationer som deltagit i undersökningen uppger att de på ett eller annat sätt har system för att övervaka och logga händelser som intrångsförsök och liknande. Det som kan anses vara anmärkningsvärt är att organisation C och E däremot anser sig ha löst loggning och övervakning av systemen via sina driftpartners.

Vi hade övervakning redan innan och vår leverantör hade infört övervakning redan tidigare […]
– Organisation E

Alla organisationer som deltagit, förutom organisation A, berättar att de har jobbat med anonymisering/pseudonymisering på ett eller annat sätt under PuL, antingen för att de kanske inte behöver personuppgifterna i ett visst fall eller för att ha möjlighet att spara data under längre tider än vad de får göra enligt avtalen.

Ja absolut. Vi anonymiserar information i vissa lägen. T.ex. i vårat BI-system. Och det kommer vi säkert att göra fortsättningsvis också.
– Organisation E

Och när kunden då väljer att avsluta sitt medlemskap då finns medlems-id:et kvar i tabellerna och all annan personuppgiftsdata stjärnmarkeras, så då blir det väl någon forma av pseudonymisera.
– Organisation C

För att ha möjlighet att bistå kunden med registerutdrag säger två av organisationerna, organisation A och C, att kunden själv kan gå in och se sin information. Alla organisationerna uppger att den registrerade har möjlighet till registerutdrag och korrigering av uppgifter via deras respektive kundtjänst.

Ja, dels kan man göra en egen export av sina köp så att säga. Och sen har vi ju en intern process där vi kan bistå kunden att ta ut den informationen.
– Organisation C

Säkerhetskopior är något som alla organisationer uppger att de har redan under PuL. Intervjuerna beskriver dock inte något konkret om hur deras schema för säkerhetskopior ser ut mer än att det kommer på tal när säkerhetskopior diskuteras i förhållande till rätten att bli bortglömd.

5.2.2 Vad har ni behövt förändra till införandet av GDPR?

Hur de olika organisationerna har arbetet inför GDPR och vad de lagt fokus på varierar såklart, men något som alla respondenter påpekar är att de inte kommer vara helt färdiga med förberedelserna den 25e maj 2018 då GDPR träder i kraft och att de till stor del även arbetat med processer, rutiner och utbildningar. Organisation A kommenterar att de inte kommer vara färdiga till införandet så här,

> *Det är nog ingen som gör det riktigt, jag vet inte det är nog väldigt få som är GDPR kompatibla här den 25e, men det är ju inte att man tar lätt på det, utan det pågår ju ett intensivt arbete här […]*
> – Organisationen A

De förändringar som organisationerna uppger att de förändrar för att ge konsumenterna information kring behandlingen och insamlandet av samtycket är uppdaterad villkor och hänvisningar till de på deras respektive hemsida. Organisation D uppger att de även kommer att förändra så villkoren skrivs under med en digital signering.

> *Det vi kommer att göra i framtiden det är att vi kommer ha en digital signering då, mellan konsumenten och oss som företag. Att du signerar det avtalet digitalt […]*
> – Organisation D

Organisation A uppger att de inför GDPR troligtvis kommer att införa en portal på deras hemsida där den registrerade har möjlighet att begära olika typer av aktiviteter, t.ex. registerutdrag, rättelse eller radering av uppgifter. Att använda sig av en webbportal för den typen av begäran vekar inte några av de andra organisationerna ha för avsikt att införa. Det som dock organisation C har är att den registrerade redan idag kan se sin information via deras hemsida och därmed även ha möjlighet att utföra några av de aktiviteterna.

> *[…] förmodligen så kommer vi ha en portal, där man fyller i ett formulär i princip, det är ett sätt då va. […] Där man fyller i information i ett formulär och den typ av förfrågning det gäller, om det är portabilitet, utdrag, korrigering av information, det är ett ganska smidigt sätt som vi tror kommer fungera bra för oss.*
> – Organisation A

I GDPR står det explicit om säkerhetsåtgärder som kryptering och pseudonymisering. Det är något som märks att de intervjuade företagen har tagit på allvar, då flera av organisationerna har sett över hur de hanterar de bitarna. Till exempel har organisation A påbörjat en översyn av vilka uppgifter som bör vara krypterade, där har de inte fattat beslutet att börja kryptera allting ännu, utan fokuserar på känsliga personuppgifter.

> *[…] det vi tittar på då, med kryptering, det är ju känsliga personuppgifter framförallt då. Vi har inte fattat det beslutet att vi ska kryptera personuppgifter, så att säga, normalt sätt utan i dagsläget är det känsliga personuppgifter som krypteras och lagras*

behörighetsskyddat då […]
– Organisation A

Organisation D har beslutat sig för att kryptera mer data som lagras än tidigare och organisation E har tagit beslut att kryptera information när de skickar den till externa aktörer.

[…] vi nycklar mer data idag än vad vi gjort innan, alltså vi krypterar mer data idag än vad vi gjorde innan.
– Organisation D

[…] där ser vi ju över hur vi skickar information till externa aktörer. Och den informationen kommer vi ju att kryptera.
– Organisation E

Som nämnts tidigare är det bara organisation A som under PuL inte har jobbat med anonymisering eller pseudonymisering. De uppger dock att det är något som de kan komma att göra under GDPR, då de anser att det ställer helt andra krav.

Det är ju helt andra krav, så det här måste vi, gallring, anonymisering, pseudonymisering, Det beror ju lite på det interna behovet också, och vad vi vill använda informationen till.
– Organisation A

En annan säkerhetsåtgärd som är återkommande mellan de olika respondenterna är jobbet med behörighetskontroller i systemen. Organisation A, B, D och E uppger att det är något som de jobbar med. Organisation E kommenterar det på följande vis:

Vi försöker ju hålla uppgifterna privata och vi försöker minimera åtkomsten till uppgifterna och sådär.
– Organisation E

Organisation A kommenterar behörighetskontroller i förhållande till GDPR på följande sett:

Att rätt personer kommer åt det. Och det är ju det som GDPR gör nu egentligen, och det stärker ju upp det ganska rejält. Det är någonting som vi tittar på med olika behörighetslösningar.
– Organisation A

När det kommer till dataportabilitet har organisationerna valt lite olika vägar. Organisation B och D säger att den delen av GDPR inte är helt definierad och kommer därför inte att erbjuda något sätt för den registrerade att få dataportabilitet. Organisation B och D säger följande:

[…] jag vet inte riktigt hur vi ska hantera den. Däremot kommer vi definitivt kunna göra utdrag på alla uppgifter som finns i klassiska PDF och sådan här format.
– Organisation B

Vi kommer initialt börja med papper, kommer vi börja. Vi kommer då printa ett litet dokument som kommer att skickas till konsumenten i pappersform.
– Organisation D

Däremot har organisation C och E implementerat tekniska lösningar och rutiner kring hur de ska hantera dataportabilitet. Organisation C säger sig ha stöd för det eftersom att de exporterar data i textfiler medan organisation E har stöd för det genom att manuellt skapa XML-filer om en kund skulle begära det.

> *[…] alltså vi levererar ju det i textfiler, sen är det ju ingen data som går att föra in i något annat system, det finns liksom ingen praktisk mottagare. Men visst de får det i ett portabelt format.*
> – Organisation C

Flera av organisationerna uppger att de jobbar med att utbilda medarbetare för missbruksregelns försvinnande. Utöver utbildande är det lite varierat hur de arbetar med att minimera spridningen av personuppgifter i ostrukturerade material. Organisation C uppger att de kommer jobba med länkar till uppgifter istället för bilagor, vilket i synnerhet gäller e-post. Organisation D kommer även de arbeta med lösningar kring e-post, men det gäller främst maskering av t.ex. personnummer som skickas.

> *Att man har personuppgifterna i en källa och man skickar länkar till den källan då. Sen får man radera källdatat när det inte är relevant att behålla det längre. […] Så främst har vi tänkt i och med ostrukturerad information har vi främst fokuserat på e-mail och samma sätt med kunders information […]*
> – Organisation C

> *Vi har då lagt ett filter då på all vår mailkonferens, så att allting som har med personuppgifter att göra, alltså ett vad blir det då, ett 14-ställigt eller 10-ställigt nummer kommer ju då att larma och maskas inom ramen för e-posten.*
> – Organisation D

Organisation A däremot jobbar med att försöka inventera och ha kontroll över vart i organisationen de har personuppgifter. De säger att de kollar på en mjukvara som de eventuellt ska införa i verksamheten som ska skanna av efter personuppgifter.

> *[…] vi tittar till exempel här på en kombination då, till ett antivirusprogram som faktiskt håller koll på klienterna lite grann, ja skannar system efter personuppgift.*
> – Organisation A

Om en kund vill utnyttja sin rätt till radering och bli bortglömd, då har alla de intervjuade organisationerna stöd för att radera information som de har i sin kundklubb. Dock när den rätten ställs i förhållande till säkerhetskopierad data är det bara organisation D som uppger att de har en färdig lösning för att inte läsa tillbaka bortglömda konsumenter.

> *Om vi skulle få en krasch i vårt centrala system och vi skulle behöva läsa på en backup av något slag, då finns det ett program som läser av om konsumenten finns med eller inte finns med. Som ligger då i ett tredje system, vilket innebär att är du med på backupen men du är inte med i den säkra kopian, de senaste sakerna, i förhållandevis till den bortglömda databasen då kommer inte konsumenten att läsas upp från backupen igen.*
> – Organisation D

En sak som har framkommit under intervjuerna är inbyggt dataskydd och dataskydd som standard. På det området uppger majoriteten av respondenterna att de inte hanterar inbyggt

dataskydd på något speciellt sätt. Respondenterna för organisation A och D uppger dock att de försöker arbeta efter de principerna nu i och med GDPR genom att införa sådana rutiner.

> *[…] men det är en sådan del som vi lyfter och kommer att införa rutiner. Vi har ju tagit fram en helt ny karta över vårt informationssäkerhetsarbete egentligen då, där också det här är en viktig del i det då.*
> – Organisation A

> *Men i allt nytt vi bygger nu, så kör vi det privacy by design […]*
> – Organisation D

5.3 Resultat från samtyckessavtal

I det här kapitlet presenteras resultatet från samtyckessavtalen för de organisationer som har intervjuats. Det görs i enlighet med de tidigare nämnda punkterna från metodkapitlet tillsammans med en analys som återkopplar till bakgrundteorin.

5.3.1 Organisation A

I medlemsvillkoren för att bli medlem i organisation As kundklubb innehåller olika typer av information. Det framgår att den registrerade när som helst kan säga upp sitt medlemskap med omedelbar verkan. I villkoren framgår det att de personuppgifter som behandlas vilka t.ex. är namn, personnummer, kontaktuppgifter och transaktionshistorik med koppling mot kundnumret. Det framgår att de behandlas när köp genomförs, för att kunna administrera medlemskapet och för marknadsföring. Villkoren nämner att personuppgifter kan komma att delas med tredje part i marknadsföringsändamål och då upprättas biträdesavtal. Den lagliga grunden som de grundar sin behandling på är för att uppfylla det avtal som de inlett med konsumenten.

Den registrerade får information om dennes rättigheter till t.ex. komplettering och korrigering av uppgifter, i vissa fall rätt till radering av uppgifter och även till dataportabilitet. Utöver det får även den registrerade möjlighet att frånsäga sig utskick av marknadsföring.

I villkoren finns en hänvisning till deras integritetspolicy för mer detaljerad information om hur de behandlar personuppgifter. Utöver det som redan beskrivits lägger de till att de vidtar relevanta säkerhetsåtgärder som t.ex. åtkomstkontroll till personuppgifterna. De tar även upp att brandväggar och antivirusprogram förhindrar obehörigt intrång i deras nätverk.

Baserat på de villkoren som konsumenten får godkänna bör organisationen ha tekniska lösningar för att uppfylla en del nya delar i GDPR eftersom att de ger konsumenten den informationen. De tar även upp att de har en viss typ av säkerhet vilket är en del som stramas åt i GDPR då säkerhetslösningar benämns explicit.

5.3.2 Organisation B

Som medlem hos organisation B får den registrerade information om unika erbjudanden, tips och inspiration, inbjudan till olika klubbaktiviteter, tävlingar, etc. Enligt villkoren framgår det att köp registreras genom att uppge sitt personnummer samt att personnumret används för att säkerställa adressuppgifterna. I övrigt framgår det att den registrerades uppgifter behandlas för

olika typer av marknads- och kundanalyser samt för marknadsföring. Den registrerade får information i villkoren att när som helst kunna avsäga sig att få erbjudanden.

Hur lång tid som uppgifterna behandlas framgår inte mer än att både den registrerade och företaget kan säga upp medlemskapet med en månads uppsägningstid.

Det framgår inte någonting om vilka tekniska åtgärder som de använder för att skydda behandlingen av uppgifterna och inga nya bestämmelser som införs med GDPR nämns. Det står inte heller någonting som berör rättelse av felaktiga uppgifter eller möjligheten att begära ut uppgifterna som de behandlar.

5.3.3 Organisation C

Den information som ges till den som ska registrera sig är allmänt om vilka förmåner den registrerade har. De förmånerna är till exempel erbjudanden och förmåner, att uppgifter om köp och kassakvitton som genomförs sparas och behandlas för att kunna administrera kundens förmåner och till analyser. Vidare skriver de även att de kan komma att använda sig av demografiska uppgifter för affärsanalyser. De insamlade uppgifterna kan komma att lämnas ut till tredjeparter i marknadsföringssyften, men att kunder som inte vill ha reklam när som helst kan avsäga sig det.

Personnumret används för att se till att adressuppgifterna är korrekta i deras system och organisationen nämner även att de som organisation förbehåller sig rätten att rätta felaktiga uppgifter, dock ingenting om att den registrerade kan begära rättelse eller radering.

Utöver villkoren för kundklubben hänvisas konsumenten till deras integritetspolicy som de har. I den policyn framgår det ganska detaljerat vad för information de samlar in och varför, t.ex. att de behöver behandla vissa uppgifter för att kunna leverera varor till konsumenten. Det framgår även att den lagliga grunden för att behandla uppgifterna är olika ifrån fall till fall, men för kundklubben är det föra att de ska kunna uppfylla det avtal som de ingår med kunden och om kunden inte vill lämna uppgifterna kan den inte vara medlem.

Konsumenten meddelas att reklamutskick baserat på tidigare köp kan förekomma samt att de kan använda uppgifterna för analyser. Uppgifterna som de samlar in behandlas för klubbmedlemmar i upp till 24 månader, efter den senast gjorda interaktionen, för att kunna skicka ut marknadsföring. Den registrerade får information kring sina rättigheter vilket omfattar registerutdrag, dataportabilitet, rättning och komplettering av uppgifter och i vissa fall rätt till begränsning och invändning mot behandling.

Organisationen medger att tredje part kan få ta del av uppgifterna om det gäller IT-leverantörer, leveranser av produkter och marknadsföring.

Organisationen uppger i policyn att brandväggar och lösenordsskydd används som säkerhetsåtgärder för att säkra upp mot intrång. Även kryptering används vid kommunikation över internet.

Organisation C har detaljerade villkor med tillhörande integritetspolicy. De dokumenten tar upp nya saker i GDPR som t.ex. dataportabilitet. Säkerhetslösningar som kryptering benämns vilket är en del av de saker som benämns i GDPR. Det tyder alltså på att organisationen har tekniska lösningar för uppfyllandet av GDPR.

5.3.4 Organisation D

I medlemsvillkoren för organisation Ds kundklubb framgår det att de behandlar personuppgifter som konsument självmant lämnat samt det som samlas in vid köp. De behandlar uppgifterna i kundklubben i syfte om att administrera medlemskapet samt för generell och riktad marknadsföring. De uppger att uppgifterna som behandlas inte kommer komma att säljas eller överföras till annan part.

Den registrerade får uppgifter om dennes rättigheter, vilka är registerutdrag, rättelse av uppgifter samt rätten att frånsäga sig direktmarknadsföring.

I villkoren står det ingenting om tekniska detaljer eller om nya fenomen som kommer till i och med GDPR. Organisation D kan i och med deras villkor uppfattas som att de inte har de tekniska lösningar som krävs för att uppfylla GDPR. De verkar däremot ha möjlighet att uppfylla delar av PuL genom t.ex. registerutdrag.

5.3.5 Organisation E

Medlemsvillkoren för att bli medlem i organisation Es kundklubb består av en integritetspolicy som beskriver behandlandet av personuppgifter och en generell del som beskriver allmänt om vad kundklubben går ut på. Den informationen som lämnas i den generella delen omfattar insamlandet av köphistorik, bonussystem och att klubbspecifika erbjudanden erbjuds till medlemmarna. Delen om integritet beskriver att uppgifterna behandlas enligt PuL. Det är dock begränsat med uppgifter om den registrerades rättigheter som nämns. Den registrerade får enbart veta att externa parter får ta del av uppgifterna i marknadsföringssyften och att den registrerade har möjlighet att begränsa användandet i dessa ändamål. Det framgår även att den registrerade har möjlighet att ändra sina uppgifter.

Det finns alltså ingenting som tyder på att de har anpassat sin verksamhet för GDPR. Det framgår inte heller om de har system där den registrerade har möjlighet till registerutdrag eller ens möjlighet att dra tillbaka sitt lämnade samtycke och därmed osäkert om de ens uppfyller alla delar av PuL.

6 Analys

I det här kapitlet kommer det resultat som tidigare presenterats att knytas an mot den bakgrund som har presenterats i arbetet.

6.1 Vilka tekniska lösningar har ni som organisation vidtagit för att uppfylla PuL?

Att använda sig av penetrationstestning för att förbättra sin säkerhet kan ha medfört att de redan under PuL har en hög säkerhetsnivå då de från externa parter får åtgärder som de bör lösa. Det framgår inte i intervjuerna vad ett sådant åtgärdsschema kan innehålla, men att de kollar på

kryptering, åtkomstkontroller och andra svagheter i systemen kanske inte är helt omöjligt. I GDPR står det att organisationer ska ha rutiner för att regelbundet testa sina säkerhetslösningar för att kontrollera att de fungerar och är tillräckliga (Bitar & Jakobsson, 2017; Datainspektionen, 2008; Europaparlamentets och Rådets förordning (EU) 2016/679, 2016), vilket penetrationstestning kan vara ett sätt att göra det på.

Det framgår inte under intervjuerna vilka typer av krypteringar som används för olika ändamål. Några särskilda krav på typer av kryptering specificeras inte heller i GDPR (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016) eller i Tankard (2016). Det framgår inte heller av intervjuerna om krypteringen är en standardinställning eller om det är något som är självvalt, men att det används innebär att någon har tagit ett aktivt beslut att använda kryptering.

Att organisationerna redan har en viss typ av övervakning av sina system, oavsett om det är implementerat av de själva eller av deras tjänsteleverantör, är en sak som de bör ha enligt GDPR, eftersom de ska kunna anmäla intrång som skett till Datainspektionen (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016). Det framgår inte något konkret i intervjuerna om hur de har tänkt att gå tillväga med incidentrapporteringen mer än att de ser över processer och rutiner inför GDPR för att kunna rapportera incidenter inom 72 timmar från att intrånget upptäckts.

Det är viktigt att se till att systemen i verksamheterna har en hög tillgänglighet då det ställs krav på att kunna återställa tillgänglighet inom rimlig tid. Det är något som Brink et al., (2017) nämner i sin rapport samt att det beskrivs i förordningen (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016). Att alla organisationer redan har implementerat rutiner för säkerthetskopior bör det vara en lösning för att tillgodose det kravet.

De säkerhetsåtgärder som organisationerna vidtagit under PuL tycks skilja sig en hel del mellan varandra. Kanske har det att göra med att det i PuL inte nämner några förslag på säkerhetsåtgärder som i kommande GDPR. PuL benämner säkerhetsåtgärder väldigt generellt på det sättet att lämpliga åtgärder ska vidtas (SFS 1998:204, 1998).

6.2 Vad har ni behövt förändra till införandet av GDPR?

Att flera organisationer svarar att de ser över vilken typ av information som krypteras kanske är en direkt effekt av att kryptering benämns explicit i GDPR till skillnad mot PuL. Att använda sig av kryptering är en välanvänd och testad lösning för att göra data oläslig för utomstående och eftersom att det står explicit i GDPR menar Tankard (2016) att det ska vara standardvalet för att skydda data. Tankard (2016) menar att om kryptering ska fungera som skydd i en organisation måste nycklarna till krypterad data bevaras på ett åtkomstkontrollerat sätt så att bara de som ska komma åt dem ska göra det. Han skriver även att behörighetskontroller bör appliceras i andra delar av organisationen också.

Inventerandet av ostrukturerad information i verksamheter som tidigare har haft stöd i missbruksregeln är en viktig del i GDPR-arbetet eftersom att personuppgifter kan finnas på många ställen där organisationen inte har en aning om det. Att inte ha koll på vart ens uppgifter finns i organisationen kan leda till problem då den registrerade kan vilja utnyttja sina rättigheter

i form av indraget samtycke eller rätten till radering. I de fallen måste organisationerna ha möjlighet att radera den informationen som kunden begär. Det kan även leda till att information som tidigare varit undantaget från PuL kommer nu även kommer att inkluderas i lagstiftningen (Brink et al., 2017).

Användandet av ett tredje system för att jämföra om en registrerad finns med i produktionssystemet eller ej vid återställning av säkerhetskopior kan innebära att de då har ett register över raderade konsumenter. Det skulle i så fall möjligtvis innebära att de inte uppfyller GDPR fullt ut då de eventuellt behandlar information om borttagna konsumenter (Brink et al., 2017). De skriver dock att en utredning på det området kommer publiceras den 12e maj.

Att inte alla organisationer är klara med vilka rutiner de har och kommer ha angående inbyggt dataskydd kan vara problematiskt då det är ett krav i den nya dataskyddsförordningen (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016). Bristen på rutiner kan i de fallen sätta användarens integritet på spel eftersom de principerna har som uppgift att skydda dessa i hela behandlingsprocessen, från start till slut.

Att alla organisationerna har svårt att hinna med kanske beror på att PuL ansetts vara verkningslös och att få fall av brott har lett till åtal (Svanfeldt, 2006; Sveriges radio, 2013), men att alla företag jobba febrilt med det kan kanske bero på de höga sanktionsavgifterna som de kan drabbas av om de inte uppfyller de nya kraven (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016; Krystlik, 2017; Ryz & Grest, 2016).

7 Slutsats

Det är väldigt olika hur de olika organisationerna jobbar med förändringar inför GDPR, det kanske beror på att det i många fall finns utrymme för tolkning samt att ingen IT-lösning är den andras lik. Men genom att intervjuerna har analyserats och resultatet tagits fram finns det ändå ett par gemensamma nämnare mellan de olika organisationerna. En av dessa är att alla organisationerna verkar jobba febrilt med GDPR och försöker se över sina verksamheter för att så snart som möjligt uppfylla den nya lagstiftningen, även om ingen av dem uppger att de kommer vara färdiga när den införs. Analysen av samtyckesavtalen visade att det var olika från organisation till organisation om hur detaljerade och uppdaterade de är. Eftersom att de är så vitt skilda i hur detaljerade de är går det inte att dra några större slutsatser enbart baserat på dessa. Det som dock går att se är att organisation A och C bör ha tekniska lösningar för delar av GDPR, men det går inte att konkretisera vilka typer av lösningar de har.

Huvuddelen av undersökningen bestod av intervjuer vars syfte är att besvara forskningsfrågan, baserat på dess två delfrågor. Nedan presenteras slutsatser för dessa två delfrågor.

Vilka tekniska lösningar har ni som organisation vidtagit för att uppfylla PuL?

Det är svårt att dra några generella slutsatser om vilka tekniska lösningar företag har vidtagit för att uppfylla PuL då det är väldigt olika från organisation till organisation. Men de tekniska lösningar som kommer upp under intervjuerna är:

- Kryptering av uppgifter på olika sätt
- Anonymisering/pseudonymisering av uppgifter
- Loggning av sina system

- Möjlighet till registerutdrag, rättelse av information och tillbakadraget samtycke
- Säkerhetskopior

Loggning av system, kryptering av uppgifter och anonymisering/pseudonymisering är saker som benämns i explicit i GDPR (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016) vilket även är något som Tankard (2016) tar upp. Möjligheten att återställa tillgängligheten av personuppgifter är något som möjliggörs genom säkerhetskopior. Ett par av organisationerna uppger även att de kontinuerligt arbetar med förbättring av säkerhetsåtgärder genom att de penetrationstestar sina system.

Vad har ni behövt förändra till införandet av GDPR?

För att generalisera resultatet av vilka förändringar de behövt införa, och svara på forskningsfrågan samt knyta an till undersökningens syfte, har organisationerna som deltagit i den här undersökningen förändrat följande tekniska lösningar inför GDPR:

- Åtkomstkontroller för sina system
- Mer kryptering av uppgifter
- Insamlandet av samtycke inklusive information till den registrerade i samband med det
- System och rutiner för missbruksregelns försvinnande

Något som organisationerna i allmänhet inte har infört fullt stöd för inför GDPR, som är krav, är lösningar för rätten att bli bortglömd, inklusive i säkerhetskopieringar och fullt stöd för dataportabilitet. Det är bara någon eller några enstaka uppger sig ha stöd för. Det var även en organisation som uppgav att de planerade att inför digital signering av avtalet, samt att det var flera som redan har eller planerar att införa någon typ av webbportal för aktiviteter som registerutdrag, rättelse, radering, etc. Ytterligare en sak som verkar vara bristande hos företagen som intervjuats är hur de arbetar med inbyggt dataskydd och dataskydd som standard då tre av fem organisationer uppger att de inte har färdiga rutiner för det.

Vad har företag med möjlighet att kartlägga konsumtionsvanor infört för nya tekniska lösningar för att uppfylla den nya dataskyddslagstiftningen (GDPR) i jämförelse med kraven i PuL?

För att sammanfattningsvis svara på forskningsfrågan som arbetet bygger på har företag med möjlighet att kartlägga konsumtionsvanor inför GDPR infört åtkomstkontroller och kryptering i sina system. För att anpassa sig till missbruksregelns upphörande har företagen exmepelvis infört speciella filytor för ostrukturerade personuppgifter, system som maskerar personuppgifter i e-post och programvara som inventerar personuppgifter ute i organisationen. Några av företagen inför även stöd för export av uppgifter i dataportablitetsvänliga format, fullt stöd för rätten att bli bortglömd (inklusive i säkerhetskopior), en webbportal för att tillåta användaren att själv utföra vissa av dennes rättigheter samt signering av samtycke med digital signering. Det framkommer också i resultatet att ett par av organisationerna inför rutiner för inbyggt dataskydd och dataskydd som standard för att hela tiden ha ett säkerhets- och intigritetstänk när de behandlar personuppgifter. Det företagen redan hade infört under PuL är övervakning av sina system i form av t.ex. en loggserver, rutiner och tekniska lösningar för

anonymisering/psedonymisering av uppgifter i systemen samt stöd för rättelse av information, möjlighet för den registrerade att dra tillbaka sitt samtycke och möjlighet att göra registerutdrag av behandlad information. Säkerhetskopior för att kunna återställa tillgängligheten av sina system är också något som de redan infört under PuL.

Det är svårt att dra slutsatser om hur organisationerna arbetar med tekniska lösningar för personuppgiftsbehandling och hur mycket de jobbar med kartläggning av uppgifter, vilket dock inte har varit syftet med undersökningen. I övrigt så uppger alla organisationer att de inför rutiner och processer i kombination med tekniska lösningar och utbildning av personal.

8 Diskussion

I följande kapitel kommer arbetet att diskuteras utifrån aspekterna resultat, samhällsnytta, metod och etiska aspekter.

8.1 Resultat

Anledningen att arbetet med kryptering av uppgifter har ökat för de tillfrågade organisationerna kan bero på att om en dataläcka inträffar, med krypterade uppgifter och nycklarna inte är åtkomliga, så betraktas det inte som en läcka (Krystlik, 2017). Det kan även bero på en direkt effekt av att det är en säkerhetsåtgärd som nämns explicit i GDPR (Europaparlamentets och Rådets förordning (EU) 2016/679, 2016). Anledningen till att alla organisationer uppger att de inte kommer hinna färdigt med förberedelserna kan kanske bero på att PuL inte tagits lika hårt (Poullet, 2006; Svanfeldt, 2006; Sveriges radio, 2013) som GDPR nu gör och har därför haft en gedigen att göra-lista. Hade de däremot implementerat fler lösningar under PuL hade förmodligen deras arbete hunnit längre eller till och med klart. Syftet med arbetet besvaras här genom att organisationerna inte är förberedda inför GDPR fullt ut, men att de förmodligen är på god väg då de infört flera nya lösningar. Det bevisar möjligen att det förväntade resultatet som fanns inför arbetet stämmer, att organisationerna inte hade de lösningar som krävdes för PuL och behöver därmed införa nya tekniska lösningar.

Flera av organisationerna påpekar att den stora delen av anpassningen till GDPR är organisatoriska förändringar i form av processer och utbildning av personal för att hantera det på ett säkert sätt. Men för att skapa stöd och förutsättningar till de nya processerna och arbetssätten kan även införandet av tekniska lösningar vara en del av anpassningen. Enligt den här undersökningen går det att generalisera resultatet att organisationerna har vidtagit nya tekniska lösningar för att uppfylla GDPR, det kan t.ex. vara kryptering och anonymisering av uppgifter och åtkomstkontroller till uppgifter. Utöver det så har vissa organisationer vidtagit åtgärder för att uppfylla individers rättigheter som t.ex. rätten att bli bortglömd eller rätten till dataportabilitet.

Karlström (2017) och Tankard (2016) kommer i sina respektive arbeten fram till att förberedelseaktiviteter för organisationer kan vara kryptering av uppgifter och åtkomstkontroller till uppgifter. Det är i linje med vad den här studie kommer fram till att företagen bland annat inför. Karlström identifierar även övervakning av system som en potentiell förberedelse, vilket den här undersökningen visar sig vara infört sedan tidigare. Flera

tidigare arbeten menar att det finns många likheter mellan dataskyddsdirektivet och dataskyddförordningen (Brink, Elvland, & Hansson, 2017; Mittal, 2017), vilket möjligtvis påvisas även i det här arbetet då organisationerna till viss del redan infört vissa lösningar som krävs för PuL och GDPR.

8.2 Samhällsnytta

För att sätta undersökningen i en samhällskontext kan det här arbetet ge företag, och i synnerhet mindre och/eller nystartade företag som inte har arbetat särskilt aktivt med personuppgiftskyddande lagstiftningar och därmed inte är helt med på vad som krävs för att uppfylla de bestämmelser som finns, ett stöd för deras arbete. Utöver att den kan vara ett stöd för företag kan det även bidra med information till de enskilda individerna om hur organisationer behandlar deras uppgifter, t.ex. vilka säkerhetslösningar de använder för att ha säkra systemen. Att konsumenten får veta med vilka tekniska lösningar som dennes information behandlas med är en viktig del då fler och fler organisationer behandlar information för att skapa ett mervärde för konsumenten (Spiekermann, et al., 2015). Det är även lika viktigt för företag och organisationer att de vet att de har korrekta lösningar både för att uppfylla den registrerades rättigheter och för att skydda dennes uppgifter som de vill behandla just för att skapa det där mervärdet.

8.3 Metoddiskussion

Den metod som använts i undersökningen kan anses vara bra därför att den har gett ett brett urval av svar och om något under intervjuerna har varit oklart har följdfrågor kunnat ställas, till skillnad mot om till exempel enkäter använts, där frågorna måste var mer exakta för att inte kunna tolkas på flera olika sätt. En brist med den valda metoden är att ingen pilotintervju användes. Att använda en pilotintervju hade kunnat ge mig som frågeställare en vägvisning i om det framtagna intervjuunderlaget var relevant inför de skarpa intervjuerna. Men eftersom att intervjuerna har transkriberats vart efter de genomförts har lärdom tagits av vilken typ av svar som kan förvänts och olika typer av följdfrågor har då kunnat förberedas till det definierade intervjuunderlaget. Ytterligare en brist med att ingen förstudie genomförts är att viktiga delar i GDPR kan ha missats som t.ex. mer konkret vilka tekniker och automatiserade processer som organisationer vidtar på olika områden inom t.ex. dataportabilitet, incidenrapportering, rätten att bli bortglömd och rättelse av information.

En annan brist med undersökningen är att på vissa områden var det svårt att få konkreta svar på vad organisationerna har gjort för förändringar. Det kan ha berott på att respondenterna inte hade tillräckligt med kunskap eller att jag som frågeställare inte frågade tillräckligt bra följdfrågor. För att åtgärda problemet med att respondenten inte kunde svara konkret på alla frågor hade eventuellt gått att åtgärda om flera respondenter från varje organisation deltagit, antingen i en intervjustudie eller i en fallstudie där det går att gå ännu mer på djupet på ett färre antal organisationer. Men som helhet gav de kvalitativa intervjuerna en vägvisning av vilka tekniska åtgärder som de vidtagit och därmed besvas forskningsfrågan.

Under sökandet av företag har ett tjugotal företag kontaktats varav sex stycken har svarat ja, men bara fem intervjuer har genomförts, på grund av att en respondent fick förhinder. Av de

som tackade nej var det en handfull av företagen som sa att de inte delade med sig av den informationen. Att de inte velat ställa upp på en anonym intervju på grund av det kan anses vara lite suspekt då ingen har möjlighet att identifiera de som ställt upp. På grund av bristen på företag som ville ställa upp beslutades det att använda sig av metoden att undersöka samtyckesavtal för de intervjuade organisationerna. Det kan ses som att den delen av arbetet inte riktigt har bidragit så mycket till själva studien, men har ändå använts som ett komplement. Med avtalen går det att se om en organisation bör ha lösningar för delar av GDPR, baserat på vad de skriver, men inte konkret hur de ser ut.

Intervjufrågorna är även utformade från bakgrundsteorin och berör de tekniska delarna vilket bör ge undersökningen en viss validitet. Resultatet från undersökningen anses vara tillförlitligt eftersom att intervjuerna har transkriberats på samma sett och av samma person, respondenterna har fått transkriberingen skickade till sig för att ha möjlighet att förändra, lägga till eller ta bort saker och ting och att alla transkriberingar har behandlats på ett objektivt sätt.

8.4 Etiska aspekter

Hur organisationer och företag arbetar med behandling av personuppgifter, säkerhet kring dessa och andra tekniska lösningar som är företagskritiska kan vara ett känsligt ämne att diskutera och dela med sig av. Syftet med det här arbetet är inte att kritisera och sätta dit hur organisationer och företag arbetar med införandet av GDPR, utan är snarare att ge andra företag en fingervisning på vilka tekniska lösningar som kan komma att behövas för att bli GDPR kompatibela. De lösningar som presenteras i arbetet ska inte tolkas som absoluta krav för vad som krävs därför att det kräver en större insikt i varje organisaions GDPR-arbete för att kunna ge sådana krav.

Eftersom information som framkommit i den här undersökningen kan anses känslig togs ett beslut att maskera alla möjliga variabler som kan identifiera de enskilda respondenterna och dess företag. Att göra företagen oidentifierbara bör även öka arbetets validitet eftersom respondenterna inte behöver undvika att svara på frågor som de anser vara för känsliga, även om de har haft den möjligheten. Det enda som går att säga om företagen är att de faller in i urvalskriterierna för att delta i den här studien, dvs. att de ska ha möjlighet att kartlägga konsumtionsvanor genom en frivillig registrering i en webbutik eller kundklubb. Det innebär att det finns ett stort antal företag som kan passa in i dessa kriterier och därmed bör det ej gå att härleda information till de specifika förtegen. Resultatet av den här studien är därför inget som kan skada de deltagande företagen.

9 Framtida arbeten

Inom området finns det en mängd olika arbeten som tar upp olika aspekter av GDPRs införande. Det gör att området kan anses vara lite urvattnat. Det finns dock ett par saker som kan vara intressant att undersöka vidare. Baserat på den här studien skulle det vara intressant att gå två vägar. Den ena vägen är att göra arbetet ännu mer kvalitativt i form av en fallstudie där en eller ett par organisationer undersök mer på djupet och då få svar på frågor som berör organisationers tekniska lösningar än mer konkret om hur de implementerat en viss lösning. Den andra vägen man skulle kunna gå är att försöka generalisera undersökningen genom en

enkät där alla möjliga företag och organisationer får möjlighet att svara på om vilka tekniska lösningar de har på de olika områdena.

Det kan också vara intressant att se om ytterligare ett par år hur organisationers arbete med GDPR har fortgått och hur deras tekniska förändringar har sett ut efter införandet. I ett sådant arbete skulle det vara intressant att undersöka hur organisationer arbetar med automatiserade processer för tidsintensiva åtgärder som t.ex. dataportablitet, rätten att bli glömd, rättelse av information samt även hur de kontinuerligt arbetar med sin säkerhet i framtiden.

Men eftersom att den här undersökningen har riktat in sig på företag och på den sida av myntet som måste applicera de nya bestämmelserna i sina verksamheter skulle det vara intressant att undersöka hur tillsynsmyndigheten, i Sveriges fall Datainspektionen, arbetar med området. Hur har de förändrat sin verksamhet? Har de infört nya system och tekniska lösningar för att anpassa sig?

Referenser

Article 29 data protection working party. (2017). *Riktlinjer om rätten till dataportabilitet.* Tillgänglig på Internet: https://www.datainspektionen.se/Documents/Riktlinjer%20om%20r%C3%A4tten%20till%20dataportabilitet.pdf [Hämtad 2018-03-08]

Article 29 data protection working party. (2018). *WP242 BILAGA – Vanliga frågor.* Tillgänglig på Internet: https://www.datainspektionen.se/Documents/Riktlinjer%20om%20r%C3%A4tten%20till%20dataportabilitet%20-%20Bilaga%20med%20FAQ.pdf [Hämtad 2018-03-08]

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

Bitar, H., & Jakobsson, B. (2017). *GDPR: Securing Personal Data in Compliance with new EU-Regulations.* Masteruppsats. Luleå: Luleå tekniska universitet.

Brink, J., Elvland, E., & Hansson, P. (2017). *Effekterna av GDPR: En jämförelse mellan Personuppgiftslagen och en kommande allmänna dataskyddsförordningen.* Kandidatuppsats. Halmstad: Högskolan i Halmstad.

Cate, F. H. (1995). The EU Data Protection Directive, Information Privacy, and the Public Interest. *Articles by Maurer Faculty.* Tillgänglig på Internet: https://www.repository.law.indiana.edu/facpub/646 [Hämtad 2018-05-30]

Datainspektionen. (2008). Säkerhet för personuppgifter. Tillgänglig på Internet: https://www.datainspektionen.se/documents/faktabroschyr-allmannarad-sakerhet.pdf [Hämtad 2018-03-11]

Datainspektionen. (2017a). Anmäla personuppgiftsincident. Tillgänglig på Internet: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/anmala-personuppgiftsincident/ [Hämtad 2018-02-22]

Datainspektionen. (2017b). Introduktion till dataskyddsförordningen. Tillgänglig på Internet: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/ [Hämtad 2018-03-08]

Datainspektionen. (2018a). Hantera personuppgifter i e-post. Tillgänglig på Internet: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/e-post/ [Hämtad 2018-04-10]

Datainspektionen. (2018b). Kan man straffas om man inte följer bestämmelserna i personuppgiftslagen? Tillgänglig på Internet: https://www.datainspektionen.se/fragor-

och-svar/personuppgiftslagen/kan-man-straffas-om-man-inte-foljer-bestammelserna-i-personuppgiftslagen/ [Hämtad 2018-02-19]

Datainspektionen. (2018c). Personuppgiftsansvarig. Tillgänglig på Internet: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/ [Hämtad 2018-03-09]

Datainspektionen. (2018d). Personuppgiftslagen. Tillgänglig på Internet: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/ [Hämtad 2018-02-12]

Datainspektionen. (2018e). Säkerhet för personuppgifter i e-post. Tillgänglig på Internet: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sakerhet-enligt-personuppgiftslagen/sakerhet-for-personuppgifter-i-e-post/ [Hämtad 2018-03-11]

Datainspektionen. (2018f). Samtycke enligt personuppgiftslagen. Tillgänglig på Internet: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/samtycke/ [Hämtad 2018-02-19]

Datainspektionen. (2018g). Strukturerat eller ostrukturerat? Tillgänglig på Internet: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/strukturerat-eller-ostrukturerat/ [Hämtad 2018-02-12]

Datainspektionen. (2018h). Vad menas med "behandling av personuppgifter" enligt personuppgiftslagen? Tillgänglig på Internet: https://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-menas-med-behandling-av-personuppgifter-enligt-personuppgiftslagen/ [Hämtad 2018-02-12]

Dobos, L. (2017). *Svenska företags anpassning till GDPR - Slutrapport från IDG Connects undersökning om svenska företags anpassning till EUs Dataskyddsförordning.* Stockholm: IDG AB. Tillgänglig på Internet: https://whitepaper.idg.se/idg-connect/gdpr---ar-foretagen-redo- [Hämtad 2018-02-15]

Edwards, R., & Holland, J. (2013). *What is qualitative interviewing?* Bloomsbury Publishing PLC.

Eklund, G. (2012). *Intervju som datainsamlingsmetod.* Tillgänglig på Internet: https://www.vasa.abo.fi/users/geklund/PDF/Intervjuer.pdf [Hämtad 2018-04-18]

Europaparlamentets och Rådets Direktiv 95/46/EG. (1995). Luxemburg: Europaparlamentet. Tillgänglig på Internet: http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:31995L0046&from=en [Hämtad 2018-02-19]

Europaparlamentets och Rådets förordning (EU) 2016/679. (2016). *General Data Protection Regulation (GDPR).* Bryssel: Europaparlamentet. Tillgänglig på Internet: https://www.datainspektionen.se/Documents/Dataskyddsf%C3%B6rordningen%20-%20Datainspektionen.pdf [Hämtad 2018-02-19]

Europeiska unionen. (2018). Förordningar, direktiv och andra rättsakter. Tillgänglig på Internet: https://europa.eu/european-union/eu-law/legal-acts_sv [Hämtad 2018-02-12]

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today, 24*(2), 105-112. doi:https://doi.org/10.1016/j.nedt.2003.10.001

Hedin, A. (1996). *En liten lathund om kvalitativ metod med tonvikt på intervju.* Tillgänglig på Internet: https://studentportalen.uu.se/uusp-filearea-tool/download.action?nodeId=459535&toolAttachmentId=108197 [Hämtad 2018-05-30]

Hert, P. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*, 179-194. doi:https://doi.org/10.1016/j.clsr.2016.02.006

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research, 15*(9), 1277-1288. doi:https://doi.org/10.1177/1049732305276687

Jourová, V. (2018). *Others care about your personal data – you should too*. Tillgänglig på Internet: https://www.euractiv.com/section/data-protection/opinion/others-care-about-your-personal-data-you-should-too/ [Hämtad 2018-03-22]

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

Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security, 2917*(6), 5-8. doi:https://doi.org/10.1016/S1361-3723(17)30050-7

Kuneva, M. (2009). *Keynote Speech.* Tillgänglig på Internet: http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf [Hämtad 2018-05-02]

Lotsson, A., & Dobos, L. (2016). *Allt du måste veta om GDPR: Ett redaktionellt Whitepaper om EU:s dataskyddsförordning GDPR.* Stockholm: IDG AB. Tillgänglig på Internet: http://whitepaper.idg.se/idg-connect/idg-whitepaper---gdpr [Hämtad 2018-02-15]

Mittal, S. (2017). Old wine with a new label: Rights of data subjects under GDPR. *International Journal of Advanced Research in Computer Science, 8*, 67-71. doi:http://dx.doi.org/10.26483/ijarcs.v8i7.4190

Poullet, Y. (2006). The Directive 95/46/EC: Ten years after. *Computer Law & Security Review, 22,* 206-217. doi:https://doi.org/10.1016/j.clsr.2006.03.004

Ryz, L., & Grest, L. (2016). A new era in data protection. *Computer Fraud & Security, 2016*(3), 18-20. doi:https://doi.org/10.1016/S1361-3723(16)30028-8

SFS 1998:204. (1998). *Personuppgiftslag.* Stockholm: Justitiedepartementet L6. Tillgänglig på Internet: http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204 [Hämtad 2018-02-12]

Skrivguiden. (2018). *Uppsatsens delar*. Tillgänglig på Internet: http://skrivguiden.se/skriva/uppsatsens_delar/ [Hämtad 2018-04-16]

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets, 25*(2), 161-167. doi:https://doi.org/10.1007/s12525-015-0191-0

Svanfeldt, G. (2006). Svenska företag tar lätt på pul. Tillgänglig på Internet: https://computersweden.idg.se/2.2683/1.2442/svenska-foretag-tar-latt-pa-pul [Hämtad 2018-02-09]

Sveriges radio. (2013). Få fälls för misstänkta brott mot PUL. Tillgänglig på Internet: http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5487830 [Hämtad 2018-02-03]

Tankard, C. (2016). What the GDPR means for businesses. *Network Security, 2016*(6), 5-8. doi:https://doi.org/10.1016/S1353-4858(16)30056-3

Vetenskapsrådet. (2002). *Forskningsetiska principer inom humanistisk-sammhällsventenskaplig forskning.* Stockholm: Vetenskapstådet.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering.* Berlin: Springer.

Bilaga A- Intervjuunderlag

Allmänna frågor:

- Vad har du för roll inom företaget?
    - På vilket sätt har du varit involverad i arbetet med GDPR?
- Vilka typer av personuppgifter behandlar ni?
- Hur ser fördelningen mellan in-house och outsourcing ut för er del när det kommer till behandling av personuppgifter?
    - Har ni några avtal med personuppgiftsbiträden?
- Baserar ni behandlingen av personuppgifter på andra lagar än PuL och kommande GDPR? T.ex. redovisningslagen
- Drar ni nytta av möjligheten att kartlägga konsumentens köpvanor i eran verksamhet?

Frågor angående tekniska lösningar och PuL:

- PuL nämner att när en person lämnar uppgifter ska denne få information kring behandlingen, hur hanterar ni det?
- Hur samlar ni in samtycke till behandlingen?
    - Hu har ni hanterat om den registrerade har återkallat sitt samtycke?
    - Om ni velat lagra information längre än vad den registrerade samtyckt till, har ni hanterat det på något speciellt sätt?
- Den registrerade har enligt PuL rätt att få veta vad ni behandlar för uppgifter om personen ifråga, hur har ni koll på all information ni behandlar om personen?
    - Hur kan den registrerade begära att få ut informationen?
- Hur har ni gjort för att lyckats rätta till felaktigheter i de uppgifter som ni behandlar (t.ex. på den registrerades begäran)?
- I PuL nämns det att lämpliga säkerhetsåtgärder ska vidtas för att motverka obehörig åtkomst till de behandlade uppgifterna, vad har ni för åtgärder för att uppfylla PuL?

Frågor angående förändringar till införandet av GDPR:

- Vilka är de största förändringarna ni har behövt göra inför GDPR?
- Hur ligger ni till i arbetet med GDPR?
- I GDPR ligger det på er som personuppgiftsansvariga att visa att samtycke samlats in, hur går ni tillväga för att göra det?
    - Har ni behövt förändra insamlandet av samtycke i och med GDPR, i så fall hur?
- Nu försvinner det svenska undantaget, missbruksregeln, hur har ni använt er av det under PUL?
    - Hur har ni gjort för att anpassa er verksamhet till att den regeln försvinner?
- Hur hanterar ni att ge den registrerades möjlighet till dataportabilitet?
- Rätten att bli bortglömd har i tidigare arbeten ansetts vara problematiskt, hur hanterar ni det?
    - Hur har ni löst backup-problematiken i förhållande till rätten att bli bortglömd?

- Ett krav är att man ska anmäla intrång till datainspektionen, har ni behövt förändra något för att ha möjlighet att upptäcka att intrång har skett?
- Kryptering och psedunomisering benämns explicit i GDPR som säkerhetsåtgärder, hur hanterar ni det?
    - Om ni vill lagra uppgifter under längre tidsperioder, hur går ni tillväga då?
- Har ni några rutiner kring inbyggt dataskydd (Privacy by design) i era system?
- Till sist, har du något som du skulle vilja lägga till gällande det vi pratat om?
    - T.ex. PuL, GDPR eller övrigt om tekniska lösningar