Uppsala universitet
Inst. för informatik och media

# Detaljhandelns förberedelser inför GDPR

## En fallstudie om vilka förändringar företagen behöver utföra samt deras arbete kring GDPR

*Paula Lundholm och Sandra Adolfsson*

UPPSALA
UNIVERSITET

Kurs: Examensarbete
Nivå: C
Termin: VT 2017
Datum: 2017-06-10

## Sammanfattning

Det rådande EU-direktivet som behandlar dataskydd från år 1995 är idag inte lika aktuellt som när det infördes. Det är därför i hög tid att en uppdatering kommer. I maj 2018 införs den nya dataskyddsförordningen, GDPR, som är EU:s senaste förordning. Den kommer ersätta Sveriges personuppgiftslag, PuL, som idag styr över hur personuppgifter behandlas. GDPR kommer innebära strängare lagar kring informationshantering och fler rättigheter till privatpersoner. Ett exempel är att privatpersoner kommer kunna be om att få alla data kopplad till personen raderade. Många företag erbjuder medlemskap till privatpersoner och lagrar därför kunduppgifter digitalt, vilket betyder att de påverkas av GDPR i stor grad då de måste omforma sina IT-system för att leva upp till de nya kraven.

Denna studie handlar om fyra företag och förändringarna de står inför samt hur de arbetar med de nya kraven som GDPR innebär för dem. En kravmodell skapas med en sammanställning av de nya kraven och resultatet visar sedan vilka företag som börjat arbeta med de kraven. Resultatet visar även hur långt de kommit i sitt arbete med dataskyddsförordningen och kan förhoppningsvis vägleda andra företag i hur de bör arbeta med dataskyddsförordningen samt vilka förändringar de bör genomföra för att leva upp till de nya kraven.



## Nyckelord

GDPR, General Data Protection Regulation, dataskyddsförordningen, informationssäkerhet, CRM

# Förord

Det här är en kandidatuppsats, skriven vid Uppsala Universitet under våren 2017. Arbetet har varit intressant och vi är tacksamma över att redan inneha kunskap om GDPR. Nedan vill vi tacka de som hjälpt till och gjort studien möjlig.

Vi vill tacka de fyra företag och Datainspektionen som ställt upp på intervjuer och givit oss en insikt i deras arbete.

Vi vill även tacka vår handledare Tomas Eklund som under arbetets gång gett värdefull handledning.

Uppsala, maj 2017.

# Innehållsförteckning

# 1. Inledning

Kapitlet inleds med en bakgrund till varför en ny dataskyddsförordning kommer att införas. Ett avsnitt i bakgrunden beskriver CRM *(Customer relationship management)* som förklarar vad företagen använder de lagrade personuppgifterna till. Därefter erhålls problemformulering, syfte och forskningsfrågor, avgränsningar, kunskapsintressenter och slutligen en disposition för att ge en överblick över uppsatsens uppbyggnad.

## 1.1. Bakgrund

Världen går mot ett alltmer globaliserat tillstånd, vilket betyder att företag, organisationer och myndigheter utbyter mer och mer information och känsliga uppgifter, och det sker ofta över landsgränser. Det är en av de främsta anledningarna till varför EU valt att införa den nya dataskyddsförordningen. Genom att skapa en dataskyddsförordning som gäller för hela EU kommer alla medlemsländer att vara tvungna att följa det nya regelverket och IT-säkerheten kommer förhoppningsvis då vara lika väl utformad i alla länder. Dataskyddsförordningen ger privatpersoner fler rättigheter, medan företagen får fler skyldigheter (Datainspektionen I 2017).

I maj 2018 införs den nya dataskyddsförordningen från EU, även kallad GDPR (*General Data Protection Regulation*). Alla företag kommer att påverkas av den nya dataskyddsförordningen då de behandlar data i form av personuppgifter. Det är viktigt att vara medveten om vad förändringen betyder för att kunna följa den och behandla personuppgifter med adekvat säkerhet i enlighet med GDPR.

I Sverige har vi en tolkning av det gamla dataskyddsdirektivet i form av personuppgiftslagen (*PuL).* Den nya dataskyddsförordningen kommer ersätta det äldre dataskyddsdirektivet och EU-medlemsländernas olika lagtolkningar av den. Skillnaden mellan direktiv och förordning är att direktiv är mål som länderna ska uppnå och det är valfritt hur de uppnås i form av exempelvis lagar. Förordningar däremot gäller direkt när de träder i kraft och är likadana i alla medlemsländer. EU-förordningar går före nationella lagar (EU-upplysningen 2016).

Det finns två huvudsakliga anledningar till varför den nya dataskyddsförordningen införs. Den ena är att det var en annan teknologisk era när det äldre direktivet infördes 1995. Då använde endast en procent av världens befolkning internet och idag är det hela 40 procent, en ökning på flera miljarder användare världen över (Internet live stats 2017). Den andra anledningen är för att det äldre direktivet tolkades olika av länderna ute i Europa. Fritt tolkande av en lag leder till att den appliceras på olika sätt i de europeiska länderna och det i sin tur leder till olika påföljder och olika stränga lagtillämpningar. Det har även lett till att personuppgifter i vissa länder inte hanteras lika strikt i alla europeiska länder. Ett exempel är Spanien som ofta delar ut straffavgifter till de som gör fel vid datahantering, medan exempelvis Frankrike knappt delar ut några straffavgifter alls. De organisationer som gör affärer över landsgränserna står därför inför många problem i och med de olika tolkningarna (Tankard 2016).

### 1.1.1. CRM

I dagens samhälle lagras personuppgifter på ett flertal ställen hos organisationer, myndigheter och företag genom olika medlemskap och andra tjänster. Detaljhandeln sparar uppgifter om individer när dessa binder upp sig i medlemskap hos företagen. Information om medlemmarna består oftast inte enbart av personuppgifter som exempelvis namn, telefonnummer och adress, utan företagen samlar även in data om vad medlemmarna konsumerar för att sedan göra analyser på det (Tsiptis & Chorianopoulos 2009).

Kundrelationshantering (*eng. Customer relationship management, CRM*) är till för att hantera kundrelationer som företaget har och för att se till att kunderna blir nöjda (Kostojohn, Johnson & Paulen 2011). Williams (2014) definierar CRM som en metod med stort fokus på att behålla, utveckla och utvinna maximalt värde från kundrelationen. Företagen kan vinna mycket på att använda CRM, bland annat effektivare personal, bättre kundupplevelser och ökad förståelse för sin verksamhet (Kostojohn, Johnson & Paulen 2011). CRM har ökat konkurrensen på marknaden och även hjälpt företagen att få lojalare kunder samt ökat deras vinst. Vinsten ökar genom att kunderna återkommer och spenderar mer vid varje köp (Chen & Popovich 2003).

För att genomföra CRM-analyser måste en stor mängd data från kunden användas, och den informationen är känslig. Det är därför viktigt att företag som använder sig av CRM är medvetna om den nya dataskyddsförordningen då den kommer att påverka dem. CRM kan delas in i tre huvudsakliga typer enligt Iriana & Buttle (2006), vilka är *Analytisk, Operativ* och *Interaktiv CRM*. Analytisk CRM tolkar och bearbetar kundrelaterade data och hjälper avdelningarna på företagen med att hantera kundrelationer på ett bättre sätt (Chan 2005). Det används exempelvis för att se mönster i företagens kunders köpbeteenden genom att analysera kundernas köp. Operativ CRM används för att förbättra effektiviteten i kundhanteringsprocesserna genom att anpassa relationen till kunderna (Iriana & Buttle 2006). Det kan ske genom att annonsera en kampanj via brevutskick (Chan 2005). Interaktiv CRM riktar sig in på att möjliggöra delning av kundernas information mellan olika avdelningar inom företagen som exempelvis sälj, marknadsföring- och supportavdelningarna (Iriana & Buttle 2006).

Företag som erbjuder sina kunder medlemskap använder sig av de olika CRM-typerna och som de är utformade måste företagen då analysera kundernas data. Det betyder att de måste vara medvetna om hur den nya dataskyddsförordningen påverkar dem då de måste göra om processer för att uppfylla de krav som GDPR ställer på dem.

## 1.2. Problemformulering

Innan 25 maj 2018 ska alla företag vara klara med omställningen som dataskyddsförordningen innebär. Det betyder att behandling av personuppgifter ska vara i linje med den nya dataskydds-förordningen. Med det menas att alla stora IT-system såväl som enkla Excelfiler ska ha granskats så att de inte bryter mot den nya dataskyddsförordningen (Privacyline 2017). Därför är det viktigt att alla som arbetar inom IT är väl förberedda och vet vilka förändringar som måste genomföras för att leva upp till de nya kraven som GDPR ställer på företagen.

I och med att den nya dataskyddsförordningen införs måste företagen förändra sina IT-system så att de lever upp till de nya kraven som tillkommer och som inte funnits med i PuL. Den nya

dataskyddsförordningen kommer att påverka många företag inom EU som hanterar person-uppgifter. Inriktning på detaljhandelsföretag är intressant då de använder sig av CRM, som förklarades i *1.1.1. CRM*. Det innebär att företagen som gör många behandlingar av personuppgifter påverkas mycket av GDPR och kommer behöva genomföra många förändringar för att kunna leva upp till de nya kraven.

## 1.3. Syfte och forskningsfrågor

Syftet med den här studien var att se vilka förändringar företagen anser att de behöver göra för att uppnå GDPR:s krav, men även vilka konsekvenser de upplever den kommer inbringa och hur de upplever att arbetet med den går. Forskningsfrågorna som studien ska besvara blir därför följande:

1. *Vilka förändringar anser företagen att de behöver genomföra och stämmer det överens med GDPR:s krav?*

2. *Vilka konsekvenser upplever företagen att GDPR kommer få för dem och hur upplever de att arbetet med den går?*

## 1.4. Avgränsningar

Avgränsning sker från andra EU-medlemsländer som även de påverkas av GDPR och riktar sig istället in på svenska företag inom detaljhandeln. Därmed avgränsar sig studien från företag som inte ingår i detaljhandeln även om de också kommer behöva genomföra förändringar inför dataskyddsförordningen. Inriktningen för den här studien blir fyra företag inom detaljhandeln, som alla erbjuder sina kunder medlemskap. Företag som erbjuder medlemskap har sparade kunduppgifter och hanterar ofta stora mängder personliga data om sina kunder. Det är därför intressant att få en bild av hur företagen kommer att påverkas av den nya dataskydds-förordningen i det avseende att de förmodligen kommer behöva göra många förändringar i hur de hanterar data om sina medlemmar.

## 1.5. Kunskapsintressenter

Studien bidrar till att ge en bild av hur företag inom detaljhandeln hanterar införandet av en ny dataskyddsförordning. Det blir en studie som ska öka insikter och kännedom inom området med syftet att sprida förståelse om vad GDPR är, och vad företag behöver förändra i sitt arbete med personuppgifter för att uppfylla de krav som kommer med GDPR. Därför är resultatet av studien givande för andra företag på marknaden som även de står inför ett arbete kring införandet av dataskyddsförordningen. Med utgångspunkt från resultatet kan de se hur andra företag arbetat med förordningen och vad som är viktigt att ta hänsyn till när de ska anpassa sin personuppgiftsbehandling ute på företagen. Resultatet kan även vara givande för privatpersoner då många har sina personuppgifter lagrade hos företag. Det kan därför vara intressant för dem att få en inblick i hur de blir påverkade av införandet.

## 1.6. Disposition

Uppsatsen är disponerad enligt följande kapitel *2. Forskningsansats och Metod*, som redogör för forskningsprocessen. Efterföljande kapitel *3. GDPR* med avsnittet *3.1. Direktivet 95/46/EG och Personuppgiftslagen* där det äldre direktivet och personuppgiftslagen beskrivs för att ge en bakgrund till den nya dataskyddsförordningen. I avsnittet efter, *3.2. GDPR:s skillnader från PuL*, förklaras de förändringar som kommer ske i och med GDPR:s införande i jämförelse till PuL. Sedan kommer *3.3. Datainspektionen och kravmodellen* där förändringar som företagen kommer behöva genomföra enligt Datainspektionen presenteras, följt av kravmodellen som framställs i uppsatsen. Empiridelen *4. Intervjuer* innehåller resultatet av intervjuerna med de fyra företag från detaljhandeln som ställde upp i studien. Därefter följer *5. Analys* där första avsnittet *5.1. Jämförelse mellan företagen* ger en analys av resultatet från intervjuerna som jämförs med den framtagna kravmodellen. Efterföljande avsnitt är *5.2. Företagen och kravmodellen* som med hjälp av en tabell visar vilka företag som uppfyller kraven. Avsnitt *5.3. Företagens upplevelser* analyseras företagens arbete med GDPR, hur de upplever att arbetet med dataskydds-förordningen går och andra delar av GDPR som inte är med i kravmodellen. I sista kapitlet, *6. Slutsats och Diskussion*, besvaras forskningsfrågorna och där erhålls en diskussion kring studien samt ett avsnitt över framtida forskning. Avslutningsvis hittas källförteckning och bilagor.

# 2. Forskningsansats och Metod

I det här kapitlet redovisas hur studien gått till i form av metod och forskningsansats. Kapitlet börjar med ett avsnitt som beskriver forskningsansats och strategi, följt av vilket forskningsparadigm som används i uppsatsen. Därefter kommer urval med en förklaring på varför de företag som är med i studien valdes ut, samt vilka skillnader och likheter företagen har. Efter urval kommer ett avsnitt om datainsamlingsmetodik där intervjuernas utformning förklaras samt val av respondenter. Kapitlet avslutas med analysmetod där analysen av intervjuerna förklaras, med ett avslutande stycke på hur analysen av resultatet kommer gå till.

## 2.1. Forskningsansats och strategi

Den valda forskningsstrategin är fallstudier. I fallstudier används flera källor, och de datainsamlingstekniker som vanligtvis ingår är intervjuer, observationer, enkäter och dokumentanalys (Williamson & Bow 2002, s. 111). Fallstudier valdes då det var den bästa strategin för att uppnå syftet och forskningsfrågorna som utformades i det första kapitlet. Utifrån forskningsstrategin valdes intervju som metod då en djupare kunskap eftersträvades för att få svar på frågeställningarna (Oates 2006, s. 141/ss. 45–48).

Anledningen till att fallstudie valdes som forskningsstrategi var för att få en djupare förståelse. Genom att genomföra intervjuer med personer på olika företag kunde det generera en bättre inblick än vad en bredare och mer ytlig informationsinsamling kunnat ge (Gerring 2006, ss. 45–48). Det var viktigt då det ännu inte fanns mycket dokumentation inom ämnet. Genom att genomföra fallstudier på företag inom detaljhandeln som hade medlemskap gav det en djupare förståelse för hur dataskyddsförordningen påverkar företag inom den branschen.

Typen av fallstudie som genomfördes var en explorativ studie. Det som karaktäriserar explorativ studie är att frågeställningarna inte är så precisa (Oates 2006, s. 143). Den här typen av fallstudie används om det finns lite eller ingen litteratur att hämta information ifrån. Då den nya dataskyddsförordningen ännu inte trätt i kraft så fanns det inte mycket litteratur att hämta fakta från. Studier hade inte heller genomförts på det valda området när det kommer till EU:s nya dataskyddsförordning. För att besvara forskningsfrågorna genomfördes fallstudier ute på fyra företag. Med hjälp av teorin och kravmodellen som framställdes så analyserades resultatet av intervjuerna på företagen. Då endast ett fåtal företag intervjuades är slutresultatet inte beskrivande eller förklarande, utan resultatet representerar hur vissa företag på marknaden hanterar förändringarna som kommer med dataskyddsförordningen och hur de skiljer sig från varandra.

## 2.2. Forskningsparadigm

Den här studiens forskningsparadigm klassas som interpretivism. Interpretivism är ofta kopplat till kvalitativ forskning. Då intervjuer användes som metod i den här studien betyder det att kvalitativa data samlades in. Filosofin bakom interpretivism är som Walsham nämner i sin vetenskapliga artikel "*...our knowledge of reality is a social construction by human actors.*" (Walsham 1995, s. 376), vilket betyder att varje individ har sin syn på verkligheten. Kriterier för interpretivism och det som genomsyrar den här typen av forskningsparadigm är att olika

individers synsätt måste tas i beaktning (Oates 2006, s. 292). Vid intervjuer är det personer som berättar utifrån sin syn och därför måste resultatet ses på kritiskt. Interpretivism karaktäriseras av att det inte finns någon absolut sanning. Det bygger bland annat på citatet i det tidigare stycket från Walsham. Eftersom alla människor har sin verklighet och sitt synsätt, så finns det inte endast en sanning (Oates 2006, s. 292). Kopplat till ämnet och forskningsfrågorna som presenterades i den här uppsatsen så kan olika företag inom detaljhandeln uppleva arbetet med dataskyddsförordningen olika och därför kan det vara svårt att dra generella slutsatser till hela detaljhandeln. Anställda på olika företag kan ha mycket skilda uppfattningar om dataskydds-förordningen och det måste tas i beaktning. Objektivitet är även viktigt och är ett kriterium för interpretivism, vilket betyder att intervjuerna och framställandet av uppsatsen har skett utan partisk syn.

## 2.3. Urval

Initialt var planen att genomföra många intervjuer inom ett företag för att få den breda och djupa kunskap som eftersträvades. Då många av företagen arbetade intensivt med förberedandet inför GDPR var det svårt att få tag på företag som kunde avsätta tid för intervju. Då inget företag kunde erbjuda intervjuer med fler än en anställd, var det enda alternativet att genomföra intervjuer med flera företag för att få en tillräcklig empirisk grund. Ett krav på att företagen skulle ha kundrelationshantering ställdes vid sökandet av företag till studien. Ett tjugotal av de största företagen inom detaljhandeln i Sverige som erbjuder sina kunder medlemskap kontaktades. Men endast fyra företag svarade och hade tid för att ställa upp på intervju. Datainspektionen, tillsynsmyndighet i Sverige, kontaktades även för att få en överblick över hur de uppfattat att företagen hanterar anpassningen till GDPR. Deras intervju användes sedan som underlag för den kravmodell som skapades i kapitel *3.3.2. Kravmodell* och som senare användes i analysen.

Vad som skiljde företagen åt var vad de erbjöd sina kunder i form av produkter. Ett av företagen säljer varor för hemmet, ett annat matvaror, det tredje företaget säljer kläder och det fjärde företaget säljer skönhetsprodukter och lämnar även ut receptbelagda mediciner. Det alla företagen har gemensamt är att de erbjuder sina kunder medlemskap i form av kundklubbar, vilket betyder att de alla använder sig av CRM och därför utför personuppgiftsbehandling. Två av företagen ingår även i samma koncern, vilket betyder att de har ett gemensamt program för arbetet med GDPR. Företagen skiljer sig dock från varandra då det i varje företag är olika team som har huvudansvaret för arbetet kring dataskyddsförordningen.

## 2.4. Datainsamlingsmetodik

Intervju var den mest lämpade metoden för studien, för att ge en djup kunskap inom området (Oates 2006, s. 141). Istället för att göra en bred och ytlig insamling av information anser Oates (2006) intervjuer som ett bättre tillvägagångssätt för att få djupare kunskap, då specialister inom området kan väljas ut. Vid intervjutillfället berättar specialisterna mer djupgående om ämnet och deras syn på det. Det leder till djupare förståelse om hur företagen inom detaljhandeln förbereder sig för den nya dataskyddsförordningen och vilka förändringar de står inför. "Specialisterna" i den här studien blev då chefer som arbetade med införandet av GDPR på respektive företag.

### 2.4.1. Utformning av intervjuer

Intervjuerna som genomfördes under fallstudierna ute på företagen var semi-strukturerade. Alternativet att använda strukturerade intervjuer ansågs inte lämpligt under fallstudierna. Anledningen var att de inte var lika djupgående som semi-strukturerade intervjuer och att det inte gick att anpassa frågorna efter situationen. Det naturliga valet var därför att välja semi-strukturerade intervjuer då Oates (2006) nämner att de flyter på bättre, kan anpassas vid intervjutillfället och även ger mer djupdykande svar. För att analysen skulle bli bra var det viktigt att få mer djupgående svar för att få en bättre förståelse. Metoden var även bra då respondenten tillåts tala fritt men med viss struktur för att inte samtalet skulle hamna i fel riktning som inte var av intresse för studien. Barriball et al. (1994) nämner att semi-strukturerade intervjuer är bra då språket kan anpassas om något missförstånd skulle uppstå eller om respondenten skulle missförstå en fråga, vilket var ytterligare en faktor som talade för intervju som metod.

DiCicco-Bloom och Crabtree (2006) talar för att skapa grundfrågor vid användning av semi-strukturerade intervjuer som en utgångspunkt vid intervjuer, vilket gjordes inför intervjuerna i den här studien. De frågorna var utgångspunkten för intervjun och andra frågor lades till beroende på svaren de genererade. Respondenten fick även leda ordningen på frågorna och därför skilde sig respondenternas intervjuer från varandra i form och upplägg (Oates 2006, s. 188). För att undvika att missa nya infallsvinklar samt att hålla frågorna öppna och objektiva, men ändå inom ramen för studien, så var semi-strukturerad intervju den bästa metoden. Intervjuerna var utformade så att en av intervjuarna hade ansvar för att ställa frågorna till respondenten och den andra var ansvarig för tekniken. Teknikansvarig innebar att se till så att inspelningen var igång samt att under intervjuns gång ta anteckningar av vilken känsla respondenten förmedlat, genom exempelvis tonläge eller andra utstickande observationer som bör dokumenteras. Respondenterna förbereddes även inför intervjuerna genom ett utskick av de förbestämda basfrågorna som låg som grund för intervjun. På det sättet kunde de förbereda sig på intervjun och vara förberedda på vad de skulle svara på för typ av frågor inför intervjuerna. Tiden för intervjun blir även effektivare då respondenten inte behöver fundera så mycket på oväntade frågor (Oates 2006, s. 189). Strukturerad metod användes i ett av fallen då mailintervju var det enda alternativet de hade att erbjuda. Utformningen av intervjun med Datainspektionen var med utgång från det underlag som presenterades på deras hemsida samt vilka frågor som ställdes till de andra intervjuobjekten. Då ett av målen med den här studien var att jämföra resultatet av intervjuer mellan Datainspektionen och företagen inom detaljhandeln var frågorna utformade efter vad Datainspektionens syn på GDPR och hur företag inom detaljhandeln hanterade övergången.

Något som eftersträvades vid intervjuernas analys och genomförande var mättnad (*eng. saturation*). Mättnad uppstår när ingen ny information kommer från intervjuerna. Vid det tillfället kan analysarbetet påbörjas och om det inte uppnås kan ytterligare en intervju behöva genomföras. Enligt Fusch och Ness (2015) uppnås mättnad när nya kategorier och teman inte längre uppstår vid kodning av intervjuer. Antalet respondenter avgör inte hur bra mättnad de insamlade data får, en stor mängd intervjuer kan producera tunga data utan innehåll (Fusch & Ness 2015, s. 2). Mättnad uppnåddes till stor grad då nya kategorier inte uppstod i de senare intervjuerna. De intervjuade företagen hanterade förberedelserna på olika sätt och därför tillkom ny information vid samtliga intervjuer, men inte tillräckligt utstickande för att inte uppnå mättnad.

### 2.4.2. Val av respondenter

Den första intervjun genomfördes med en anställd på Datainspektionen. Där fanns ingen möjlighet till att få varken en personlig intervju eller en telefonintervju och därför var alternativet att genomföra en strukturerad intervju via mail. "Frågor och svar" från Datainspektionens hemsida, som är framtagen för att svara på vanliga frågor ställda av företag och privatpersoner gällande dataskyddsförordningen, användes också. Datainspektionens intervju ligger som underlag till den kravmodell som presenteras i *3.3.2. Kravmodell* och finns därför inte med de andra intervjuerna i kapitel *4. Intervjuer*. Ett tjugotal företag inom detaljhandeln kontaktades inför den här studien. Där eftersöktes respondenter på företagens IT-avdelningar med roller inom CRM och säkerhet som hade koppling till arbetet med GDPR. Urvalet av respondenter var inte stort då många av de företagen som kontaktades var mycket upptagna med den nya dataskyddsförordningen. Därför har endast en respondent på företagen valts ut för att svara på frågor. De som erbjöd sig att ställa upp på intervju var alla chefer av något slag. Respondenterna skiljer sig från varandra i det avseende att de har olika typer av chefsroller inom respektive företag.

Fem intervjuer genomfördes med en respondent på respektive organisation (se Tabell 1). Initialt var tanken att alla intervjuer skulle ske genom personliga (*face-to-face*) intervjuer. Då det var problem med att få personer att ställa upp på intervjuerna erbjöds intervju genom telefon som alternativ. Personliga intervjuer är att föredra då respondentens kroppsspråk, ansiktsuttryck och andra detaljer som kan uppfattas vid personlig kontakt kan analyseras. Tidigare forskning på skillnader mellan personlig intervju och telefonintervju har dock gjorts och den har visat att det inte är någon stor skillnad på de två intervjuformerna (Sturges & Hanrahan 2004, s. 112).

| **Företag** | **Respondent** | **Roll** | **Intervjutyp** | **Tidsåtgång** |
|---|---|---|---|---|
| Datainspektionen | Martin Brinnen | - | E-mail | - |
| Företag 1 | Respondent A | CRM-chef | Telefonintervju | 18 min |
| Företag 2 | Respondent B | Strategisk IT-chef (CIO) | Telefonintervju | 15 min |
| Företag 3 | Respondent C | Projektledare IT-avdelning | Telefonintervju | 20 min |
| Företag 4 | Respondent D | Data Protection Officer | Telefonintervju | 20 min |

Tabell 1 - Lista över respondenter

## 2.5. Analysmetod

Litteraturundersökning ger en stabil informationsgrund. En översiktlig bild samlas in som är av vikt innan en mer djupare datainsamling sker. Med en bra litterär grund ökar intervjuerna i kvalité. Ordningen som allt utförs i, samt förberedelser för utförandet, är därför en betydelsefull del av forskningsprocessen (Dimond 2015).

En kvalitativ dataanalys genomfördes på resultatet från intervjuerna. Enligt Dimond (2015) bör analysen börja direkt efter att intervjun är över då det är enklare att reflektera över användbara teman, vilket gjordes i den här studien. Respondenterna spelades in under tillfället intervjuerna genomfördes för att sedan transkriberas. De transkriberade dokumenten lästes sedan igenom för att få en överblick över innehållet. Efter genomgången av dokumenten identifierades olika teman. Oates (2006) nämner tre olika teman där det första är sådana segment som ej är relevanta för forskningsfrågan. Det andra temat är sådant som är viktigt för att förstå kontexten och det tredje är sådana segment som är direkt viktiga för själva forskningsfrågan. Genom att använda teman kunde information som inte var direkt relevant för forskningsfrågorna och syftet av studien sållas bort. När temana var valda så skulle kategorier väljas. Kategorierna valdes via induktivt tillvägagångssätt, vilket betyder att kategorierna inte var förvalda utan valdes ut efter arbetets gång. Kategorierna som hade många nyckelord delades sedan upp i fler kategorier. Efter uppdelandet parades de ihop med teman (Oates 2006, ss. 268–270). Då förändringarna för företagen var en stor del av studien så var ”förändringar” och “konsekvenser” två löst förvalda kategorier som utgicks från i början vid intervjuerna. Det var svårt att välja kategorier innan första intervjun genomförts då ingen litteratur kunde visa på hur det såg ut i detaljhandeln inom det här området. Men genom att ha de två ovannämnda kategorierna fanns det något att utgå från. Det var viktigt vid dataanalysen att inte utgå från egna teorier. Det hade kunnat påverka analysen negativt och kunnat ge en feltolkning av de kvalitativa data (Oates 2006, s. 275).

För att analysera resultatet av intervjuerna så skapades ett ramverk i form av en kravmodell. Ramverket är tänk att ligga som grund för andra företag för att veta vilka krav GDPR ställer på dem. Det baseras på vilka förändringar Datainspektionen ser att företagen måste genomföra, samt krav som GDPR ställer på dem. Kravmodellen innehåller punkt för punkt en förkortning av kraven, en förklaring över vad de betyder samt källa till kravens ursprung. Kravmodellen analyseras sedan efter kraven som kravmodellen nämner mot vad respondenterna på företagen berättat att de arbetar med för förändringar.

Det är viktigt att resultatet från intervjuerna går att bekräfta i efterhand (Oates 2016, s. 294). Dokumentationen från intervjuerna var därför viktig för att andra efteråt ska kunna gå igenom det och intyga att det finns en grund för det slutgiltiga resultatet. Intervjuerna transkriberades vilket stärker det som sagts under dem. Då företagen ville vara anonyma finns inte företagens kontaktinformation tillgänglig då anonymiteten ska behållas. Fakta från litteratur är enkel att hitta då den finns med i källförteckningen. Genom dokumentationen finns det alltså tillgängligt för en andra part att styrka det slutliga resultatet som uppsatsen presenterar.

# 3. GDPR

I det här kapitlet beskrivs först det tidigare direktivet 95/46/EG samt den svenska tolkningen av direktivet i form av personuppgiftslagen. Därefter kommer en utförlig beskrivning av den nya dataskyddsförordningen, GDPR, som ersätter det tidigare direktivet. Kapitlet avslutas med en kravmodell framställd med hjälp av Datainspektionen, som är utsedd tillsynsmyndighet i Sverige, och dataskyddsförordningen.

## 3.1. Direktivet 95/46/EG och Personuppgiftslagen

I oktober 1995 infördes EU-direktivet 95/46/EG. Direktivet infördes för att skydda enskilda personer och behandling av deras personuppgifter (Europaparlamentets och rådets direktiv 95/46/EG). För att få en bättre förståelse för vad en *personuppgift* är beskrivs det i direktivet som:

> *varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet* (Europaparlamentets och rådets direktiv 95/46/EG).

Själva *behandlingen av personuppgifter* definieras som:

> *varje åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring* (Europaparlamentets och rådets direktiv 95/46/EG).

Medlemsländerna hade tre år på sig att införa direktivet i den nationella lagstiftningen. Det var i samband med införandet av direktiv 95/46/EG som förslag till PuL började arbetas fram, som sedan trädde i kraft 1998 (Datainspektionen IV 2017). Europeiska kommissionen publicerade först 2003 en rapport om hur implementationen av det nya direktivet gått. Anledningen till att det tog så lång tid att ta fram rapporten berodde på att flera medlemsländer hade stora fördröjningar vid införandet av direktivet. Vid rapportens publicering var Frankrike det enda medlemsland som ännu inte hade implementerat det nya direktivet (Korff 2002).

Målsättningarna med att införa ett gemensamt direktiv var bland annat att upprätta närmare relationer mellan EU:s medlemsnationer och säkerställa ekonomiska och sociala framsteg i länderna. Det skulle ske genom gemensamma åtgärder för att undanröja barriärer som gör det svårare för ett utbyte av data länder emellan. I samband med införandet kunde inte längre medlemsstaterna hindra det fria flödet av personuppgifter mellan dem, då de alla fick ett likvärdigt skydd av personuppgifterna (Europaparlamentets och rådets direktiv 95/46/EG). En viktig del i direktivet var införandet av artikel 29-gruppen som består av en representant från varje medlemsland, en eller flera representanter utsedda av EU-institutionen och en representant

från Europakommissionen. Namnet kommer från artikel 29 i direktivet och gruppens arbetsuppgifter beskrivs i artikel 30. Gruppens huvudansvar är att se till att direktivet ser likadant ut i alla medlemsländer. De har även ansvar över att hålla Europakommissionen uppdaterad om hanteringen av personliga data ser ut i medlemsländerna genom rapporter, undersöka hur direktivet efterföljs och ge råd om tillägg till direktivet (Europaparlamentets och rådets direktiv 95/46/EG).

Idag är det personuppgiftslagen (*PuL*) som finns till för att skydda människors personliga integritet. 1998 trädde PuL i kraft och är den svenska implementering av EU:s dataskyddsdirektiv 95/46/EG. Lagens syfte är att *"skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter"* (SFS 1998: 204). Den som behandlade personuppgifter fick i samband med PuL:s införande ett större ansvar för att se till att behandlingen var laglig (Datainspektionen IV 2017). Den nya dataskyddsförordningen kommer ersätta personuppgiftslagen och därför kommer stora förändringar behöva ske i hur företagen hanterar personuppgifter (Dataskyddsförordningen I 2017).

## 3.2. GDPR:s skillnader från PuL

General Data Protection Regulation (*GDPR*), eller dataskyddsförordningen som den kallas här i Sverige, kommer bestå av en EU-förordning som gäller alla utom polisen, och ett EU-direktiv som gäller endast polisen (samt andra brottsbekämpande myndigheter). Den nya dataskyddsförordningen tillåter att enskilda individer ska kunna vända sig till respektive lands tillsynsmyndighet med klagomål gällande uppgifter som hanteras i ett annat land. Det medför att samarbetet mellan myndigheterna inriktade på dataskydd i EU:s medlemsstater kommer bli mycket starkare än tidigare (Datainspektionen III 2017).

Huvudmålet med GDPR är att förstärka privatpersoners rättigheter och ge dem större kontroll över sina personuppgifter. Det innebär att privatpersoner bland annat kommer ha rätt att be företagen om att få alla data kopplad till dem raderade (Datainspektionen I 2017). Nedan kommer de förändringar som dataskyddsförordningen innebär och som skiljer sig från PuL.

Rätt till rättelse, privatpersoner kommer kunna höra av sig till företagen för att rätta de personuppgifter som finns registrerade och kunna komplettera ofullständiga personuppgifter (Europaparlamentets och rådets förordning 2016/679, Artikel 16). Rätten att bli raderad tillkommer också och är en av de större förändringarna. I dataskyddsförordningen kallas det även "rätten att bli bortglömd" (Europaparlamentets och rådets förordning 2016/679, Artikel 17). Det innebär att privatpersoner har rätt att få alla sina personuppgifter raderade utan fördröjning. I Pul 28§ finns en liknande paragraf, skillnaden är att den endast gäller på personuppgifter som inte behandlas enligt lag (SFS 1998:204).

Idag kan företagen välja om de vill tillsätta rollen som personuppgiftsombud. Det är inget krav enligt PuL utan kan vara till hjälp för personuppgiftsansvarig, alltså företaget som behandlar personuppgifter (SFS 1998:204). Dataskyddsombud heter den nya rollen som kommer med GDPR som ersätter personuppgiftsombuden. Skillnaden mellan dataskyddsombuden och personuppgiftsombuden är att de kommer behöva uppfylla fler krav. De organisationer som genomför systematisk övervakning eller har en omfattande behandling av känsliga uppgifter

kommer bli tvungna att tillsätta ett dataskyddsombud (Europaparlamentets och rådets förordning 2016/679, Artikel 37). Dataskyddsombudet har ansvar över att företaget det arbetar för följer dataskyddsförordningen. De har även som uppgift att ge information och råd till den personuppgiftsansvarige eller personuppgiftsbiträdet, samt relevanta anställda om vilka skyldigheter de har enligt dataskyddsförordningen. Dataskyddsombudet ska även övervaka att dataskyddsförordningen följs och på begäran ge råd gällande konsekvensbedömning rörande dataskydd. Slutligen måste dataskyddsombudet också samarbeta med och vara kontaktpunkt för tillsynsmyndigheten som i Sverige är Datainspektionen (Europaparlamentets och rådets förordning 2016/679, Artikel 39). För att ta hänsyn till de små företagens situation kommer de företag som har färre än 250 anställda inte ha en skyldighet att tillsätta något dataskyddsombud (Gutwirth, Leenes & de Hert 2015, s. 162). Med undantag om behandlingen som utförs med sannolikhet kommer medföra en risk för den registrerades rättigheter och friheter och om företagets huvudsakliga verksamhet är att behandla personuppgifter (Europaparlamentets och rådets förordning 2016/679, Artikel 30).

De behandlingar som leder till hög risk för fysiska personers rättigheter och friheter ska först genomgå en konsekvensbedömning. Den bedömningen ska utföras innan behandlingen, och ska innefatta den planerade behandlingens konsekvenser och risker för skyddet av personuppgifter. Den principen finns inte i PuL, utan är ett tillägg i GDPR (Europaparlamentets och rådets förordning 2016/679, Artikel 35).

En märkbar förändring från PuL är försvinnandet av missbruksregeln. Idag finns det en undantagsregel för behandling av ostrukturerade data i PuL (Datainspektionen II u.å.). Den gör det tillåtet att ha personuppgifter i ostrukturerat material som email eller enklare listor. Missbruksregelns försvinnande drabbar alla företag då exempelvis information om de anställda brukar mailas mellan de olika cheferna och HR-avdelningen (Langhorst & Jaibaji 2017). I och med införandet av GDPR så försvinner missbruksregeln då den nya dataskyddsförordningen inte innehåller någon undantagsregel.

Rätt till dataportabilitet är ett helt nytt krav som införs med GDPR och finns inte med i PuL. Dataportabilitet innebär att datasubjektet, den person som kan kopplas till specifika data som exempelvis namn eller personnummer, har rätt att få tillgång till sina personliga uppgifter hos en tjänsteleverantör och sedan kunna välja att överföra dem till en annan tjänsteleverantör. Data kan alltså på en privatpersons begäran byta IT-miljö. Det huvudsakliga målet med dataportabiliteten är att öka konkurrensen bland tjänsteleverantörer och öka det fria flödet av personliga data inom EU. Rättigheten att kunna flytta över personlig information är även tänkt att öka jämställdheten mellan privatpersonen och de som behandlar data. Privatpersoner kommer i och med GDPR kunna begära ut data från företag för eget bruk. Dataportabilitet beskrivs enligt följande citat från dataskyddsförordningen:

> *Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format...* (Europaparlamentets och rådets förordning 2016/679, Artikel 20, punkt 1).

Artikel 29-gruppen har tagit fram exempel på vad för information som skulle kunna begäras ut av ett företag. I rapporten ges exemplet där en privatperson kan begära ut sin spellista från en musikstreamingtjänst som exempelvis Spotify för att se hur många gånger vissa låtar spelats för att sedan köpa de låtarna från ett annat företag som säljer musik (Europeiska Kommissionen II 2016, s. 2).

Samtycken måste lämnas av den registrerade vars personuppgifter ska behandlas och kraven på hur det genomförs har blivit strängare. I PuL benämns samtycke som:

> *Känsliga personuppgifter får behandlas, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort uppgifterna* (SFS 1998:204, 15§).

GDPR har en längre förklaring än PuL på vad ett giltigt samtycke är och hur samtycket ska ges. Är det olika typer av behandlingar, ska olika samtycken ges av den registrerade. Det får inte vara en förkryssad ruta samtycket godkänns med, utan den registrerade måste aktivt godkänna behandlingen. Det står även uttryckligen att det klart och tydligt ska framgå för den registrerade vad samtycket ges till, vilket betyder att kundvillkoret, det som godkänns måste vara tydligt så att den registrerade förstår vad samtycket ges till (Europaparlamentets och rådets förordning 2016/679, Artikel 7). Thornton, arbetar som IT-chef inom tjänsteförsäljning, nämner att alla avtal med kunder måste ses över hos företagen (C5 Alliance 2017), då de som ovan nämnt behöver vara tydliga, vilket kan betyda att företagen måste omformulera dem för att de ska uppfylla GDPR:s krav. Därför kommer det bli nödvändigt att samla in nya samtycken om kundvillkoren ändras.

Idag finns det ingen paragraf i PuL som kräver att företagen ska anmäla en incident. Med GDPR införs kravet på incidentrapportering och har som krav att anmälan ska ske inom 72 timmar, utan onödig tidsfördröjning, efter att ha fått vetskap om incidenten. Anmälan sker till Data-inspektionen, dock är anmälan endast nödvändig såvida det är sannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter (Europaparlamentets och rådets förordning 2016/679, Artikel 33).

Skadestånd finns som paragraf i PuL, men nämner endast en ersättning till den registrerade för skadan och den kränkning av den personliga integriteten som brottet orsakat, ingen summa nämns (SFS 1998:204, 48§). Med GDPR kommer ett bestämt sanktionsbelopp på 20 miljoner euro eller fyra procent av företagets föregående års globala omsättning, vilket av dessa två som är högst kommer företagen få betala som straffavgift (Europaparlamentets och rådets förordning 2016/679, Artikel 83).

Det är många experter som uttalat sig om GDPR och det råder delade meningar angående hur företagen kommer hinna klart innan införandet av dataskyddsförordningen. Enligt en artikel i Computer Sweden av Finnegan (2017) nämner analysföretaget Gartner att ungefär hälften av alla företag som påverkas av GDPR inte kommer hinna klart innan införandet. I en intervju med advokaten David Frydlinger (Rosengren 2017), expert inom IT-juridik, är Frydlinger inne på samma spår som analysföretaget Gartner. Han berättar att han har svårt att se att organisationer hinner med en full förberedelse inför GDPR:s införande 2018. Han nämner bland annat att

företagen måste göra en utredning om vilka personuppgifter som behandlas och varför. Problem kan uppstå när företagen ska radera data och därför kan vissa IT-system behöva byggas om helt. En viktig del i arbetet kring GDPR är att involvera alla avdelningar då personuppgifter finns överallt inom verksamheten (Rosengren 2017). Det är inte enbart IT-avdelningen som påverkas utan Frydlinger nämner fler avdelningar som påverkas:

> *Personuppgifter finns ju överallt. Man måste ha med marknad och HR, juristavdelningen, inköp, sälj och IT-avdelningen…* - David Frydlinger (Rosengren 2017)

Thornton (2017) ser lite mer positivt på om företagen kommer hinna klart. Han säger i en intervju att om företaget följer det tidigare direktivet 95/46/EG så har de en bra bas, men att det ändå är en del nytt som måste ses över för att hålla GDPR-standard (C5 Alliance 2017). Andra problem som kan fördröja arbetet med förordningen är lagtolkning. Lagtolkning är en process att tolka en lagbestämmelse, vilket ofta är nödvändigt då lagtext alltid skrivs på ett generellt sätt. Det generella skrivsättet är för att lagarna inte kan skrivas så de reglerar alla situationer på detaljnivå (Lagen.nu 2017). Eriksson och Goldkuhl (2015) skriver följande om lagtolkning:

> *Lagar och förordningar är olämpligt formulerade. De baseras på en oklar och föråldrad begreppsbildning och är sinsemellan komplexa med därmed stor risk för att felaktiga eller snäva rättstolkningar görs.*

## 3.3. Datainspektionen och Kravmodellen

Datainspektionen är en myndighet i Sverige som ser till att personuppgifter behandlas på ett korrekt sätt i organisationer. Deras huvuduppgifter är att se till att den personliga integriteten inte kränks, att företagen uppfyller kraven för hanteringen av personuppgifter (Datainspektionen V 2017) och att PuL följs. Företag och privatpersoner som behöver hjälp med hur personuppgifter ska behandlas kan höra av sig till myndigheten.

### 3.3.1. Datainspektionen om företagens förändringar

Nedan presenteras förändringar som företagen kommer behöva genomföra enligt Datainspektionen och hur de upplever att företagen hanterar arbetet kring dataskyddsförordningen. Materialet kommer från en intervju som genomfördes med Datainspektionen och kommer användas som grund till det ramverk som framställs i efterföljande avsnitt *3.3.2. Kravmodell*.

Datainspektionen har kontakt med många företag som hör av sig till dem för att ställa frågor om dataskyddsförordningen. Den största förändringen för företagen tror respondenten kommer bli att ständigt ha uppdaterad dokumentation om hur de behandlar personuppgifter samt att informera företagens kunder på ett mer utförligt sätt i form av bland annat kundvillkor. Samtycken är något företagen har ställt många frågor om till Datainspektionen då det blir högre krav på hur det ges i och med dataskyddsförordningen. Det går inte att undvika att göra några förändringar berättar respondenten, även om företagen har bra hantering idag så måste de ändå göra en genomgång av sina system. Det är en fördel om hanteringen har varit bra tidigare, men respondenten nämner att företagen bland annat måste *"ta nytt ansvar till exempel incidentrapportering"*. Han nämner även att vissa företag kan ha missat att den nya dataskyddsförordningen kommer att ersätta PuL, som därmed slutar existera.

Inställningen till GDPR anser respondenten vara mestadels positiv, han beskriver det som att de flesta tycker det är bra med en genomgång av alla system för att få en inblick i dem och en bättre struktur.

> *Inställning till GDPR är av de flesta positivt. De tycker det är bra att det blir ordning och reda.* - Martin Brinnen

Många ser även fördelen med att det blir samma regler i hela EU, vilket det idag inte är. Respondenten anser att många företag ser förberedelsearbetet förknippat med stora kostnader och risken för att drabbas av sanktionsavgifter är oroande. Det finns också problem med att många bestämmelser i dataskyddsförordningen är oklara och att ingen har någon klar bild över hur de ska tolkas. De företag som i dagsläget inte har kontroll över vilken personuppgifts-behandling som de utför och inte har gjort överväganden enligt personuppgiftslagen kommer troligen ha de största utmaningarna. Respondenten anser att det är svårt att se om alla företagen skulle hinna klart med alla förändringar i tid men att de som börjat arbeta med GDPR med största sannolikhet kommer hinna klart till införandet 25 maj 2018.

### 3.3.2. Kravmodell

Nedan redovisas en kravmodell för vad företagen måste förändra (Tabell 2). Till grund för kravmodellen ligger Datainspektionens intervju som presenterades i föregående avsnitt samt regelverket, GDPR. kravmodellen kommer att användas i analysen för att jämföra företagens uppfattning över vad de anser att de måste förändra mot vad dataskyddsförordningen och Datainspektionen säger.

| Nya krav | Förklaring | Källa |
|---|---|---|
| Rätten till rättelse | Företagens medlemmar ska ha rätt att få tillgång till sina personuppgifter samt kunna rätta dessa och kunna komplettera ofullständiga personuppgifter. | Europaparlamentets och rådets förordning 2016/679, Artikel 16 |
| Rätten till radering | Företagens medlemmar har nu "rätten att bli bortglömd", vilket betyder att företagen måste radera alla data kopplade till medlemmen. | Europaparlamentets och rådets förordning 2016/679, Artikel 17 |
| Tillsätta ett dataskyddsombud | Det nya dataskyddsombudet ersätter det tidigare personuppgiftsombudet från PuL. Dataskyddsombudet får fler krav att leva upp till. Undantag för företag med färre än 250 anställda som inte genomför systematisk övervakning. | Europaparlamentets och rådets förordning 2016/679, Artikel 37. Gutwirth, Leenes & de Hert 2015 |
| Konsekvensbedömning | Företagen måste genomföra en konsekvensbedömning för varje personuppgiftsbehandling som innebär risker för dem som behandlingen berör, samt se vad som kan göras för att minimera riskerna. | Europaparlamentets och rådets förordning 2016/679, Artikel 35 |
| Dokumentationskrav | En ökad dokumentation kommer behöva ske i företagen. De måste börja dokumentera hur personuppgifterna behandlas. Det för att kunna visa att dataskyddsförordningen efterlevs. | Intervju med Datainspektionen |

| | | |
|---|---|---|
| Missbruksregeln | Personuppgifter som finns i ostrukturerat material som email måste tas bort. Det betyder att processer för hur personuppgifter hanteras i exempelvis supporten hos företagen måste ses över. | Langhorst & Jaibaji 2017 |
| Dataportabilitet | Företagen måste skapa processer för att kunna hantera kunder som vill flytta över sina personuppgifter till ett annat företag. | Intervju med Datainspektionen |
| Uppdaterade kundvillkor | Företagen måste uppdatera sina kundvillkor så att dessa är lättlästa och så att kunden kan godkänna varje behandling för sig. För ett företag inom detaljhandeln innebär det att se över hur kunderna informeras om hur personuppgifterna behandlas. Vid varje ny behandling måste kundvillkoren uppdateras. | Intervju med Datainspektionen |
| Samla in nya samtycken | Företagen måste samla in nya samtycken till de nya uppdaterade kundvillkoren. Samtycke måste ges inför varje behandling av personuppgifter. | Intervju med Datainspektionen |
| Incidentrapporteringskrav | Företagen måste skapa processer för hur incidentrapportering ska gå till. Måste anmäla incident senast 72 timmar efter händelsen inträffat. | Europaparlamentets och rådets förordning 2016/679, Artikel 33 |

Tabell 2 - Kravmodell över de nya kraven GDPR ställer på företagen

# 4. Intervjuer

I det här kapitlet kommer fem intervjuer att presenteras med bakgrund om respektive företag för att få en uppfattning om hur omfattande kundhantering de har samt en kort introduktion av respondenten. Därefter följer resultatet av intervjun om hur de arbetar kring den nya dataskyddsförordningen. Intervjuunderlaget återfinns i bilaga 2. Kapitlet avslutas med en sammanfattning av intervjuerna för att få en klarare syn på företagens likheter samt vad som skiljde dem åt. Företagsintervjuerna är anonymiserade och därför har viss källhänvisning, exempelvis företagens hemsidor samt företagsnamn, valts att uteslutas för att behålla deras anonymitet.

## 4.1. Företag 1

### 4.1.1. Bakgrund

Företag 1 är ett stort företag inom detaljhandeln som idag finns ibland annat Sverige, Norge, Finland, Storbritannien och Tyskland. Företaget har idag ungefär två och en halv miljon medlemmar. Företag 1 har två olika kundklubbar där den ena är för privatpersoner som finns i Sverige och Finland. Den andra är för företag och finns i Sverige och Norge. Medlemmarna kan anmäla sig till kundklubben genom att fylla i ett formulär i butik eller på deras hemsida på nätet. Formuläret låter kunden lämna sitt namn och personnummer, adress är frivilligt att fylla i då det kan hämtas från tredje part genom personnumret. I deras kundvillkor står det att uppgifterna som samlas in om köp behandlas för att *"administrera kundförhållandet"*. För att få ut det mesta av de data som sparas så använder sig Företag 1 av bland annat Interaktiv CRM. Då tillåts alla avdelningar att samarbeta och ta del av data som även kan vara av värde för andra avdelningar.

Företagets CRM-chef, Respondent A, ställde upp på en telefonintervju angående hur de hanterar införandet av den nya dataskyddsförordningen. Respondenten har arbetat 12 år inom företaget på flertal avdelningar inom sälj, inköp och kampanj.

### 4.1.2. Arbetet kring dataskyddsförordningen

Arbetet kring GDPR inleddes efter nyår genom att skapa en styrgrupp bestående av 10–15 personer från olika avdelningar inom företaget. Nyckelpersonerna kom från jurist-, marknad- och IT-avdelningarna. Marknadsavdelningen har störst antal medlemmar i den här styrningsgruppen med flest antal representanter. Arbetet började med en översättning av lagkraven för att förstå vad det rent konkret betydde för företaget. Några oklarheter finns fortfarande kvar kring dataskyddsförordningen, som frågor kring artikel 29 gruppen.

De största förändringarna som respondenten tror kommer att ske inom företaget har att göra med ändring av program och processer kopplade till medlemmarnas rätt att bli raderade och förändring av personuppgifter. Radering och förändring av personuppgifter kommer att kunna genomföras i alla kanaler beskriver respondenten, alltså i butik, online och via telefon. Företaget har idag inte mycket personuppgifter i ostrukturerade data såsom mail. Därför ses det inte som ett problem nu när missbruksregeln försvinner. Respondenten berättar att det kan förekomma på CRM- och HR-avdelningen, men inte i något större omfång som skulle innebära större problem. Hen förklarar att dokument på hur kommunikation kommer få se ut kommer tas fram.

*...det kommer säkert att bli ett dokument hur vi ska kommunicera med varandra och sådant. Det står helt klart på listan.* - Respondent A

När det kommer till dataportabilitet tror respondenten att det inte kommer bli något problem för företag inom detaljhandeln, utan det tror respondenten kommer påverka sjukvården i större utsträckning. Kassauppdateringar kommer behöva genomföras, också nya medgivanden från alla medlemmar kommer att behöva samlas in. Respondent A tror att medlemmarnas medgivanden kommer att kräva mycket resurser. När det kom till bemanning kring de uppdaterade processerna och hanteringen av medlemmar som eventuellt kommer höra av sig, var framtiden svårbedömd. Arbetet kring bemanning har ännu inte startat men respondenten spekulerade kring hur utfallet kunde bli och kom fram till att det förmodligen kommer att anställas ett fåtal personer.

Respondentens inställning till den nya dataskyddsförordningen uppfattades som positiv. Det poängteras att den lett till att alla processer granskats för att se vad de gör och om de kan förbättras. Vilket har gett en bättre inblick i företagets processer.

## 4.2. Företag 2

### 4.2.1. Bakgrund

Företag 2 är ett ganska ungt företag som är en del av en större koncern, som idag har runt 400 butiker med 3000 anställda. Företag 2 har en kundklubb där de samlar in personliga data som kunderna lämnar när de registrerar sig som medlemmar i kundklubben. Dit hör bland annat namn, personnummer, adress och betalningsuppgifter. De samlar även in information om vilka produkter kunderna köper i butik och i nätbutiken. Sedan används den informationen för att göra analyser för att skapa erbjudanden vid bland annat direktmarknadsföring. Men även för att anpassa varor och tjänster, vilket står i deras bonusvillkor. De använder sig av bland annat Analytisk CRM för att göra analyser på köphistorik men även för Interaktiv CRM då information från kunderna används för att anpassa varor och tjänster hos företaget.

Respondent B är CIO (*Chief Information Officer*) på Företag 2 och har arbetat sju år inom den större koncernen som företaget tillhör och på nuvarande position i tre månader. Arbetet som CIO innebär ett ansvar för applikationer, affärsprocesser inom IT och förvaltning.

### 4.2.2. Arbetet kring dataskyddsförordningen

Arbetet med GDPR började i januari då koncernen startade en projektgrupp mestadels bestående av parter från den juridiska sidan med advokater där projektledaren är en inhyrd konsult. Projektgruppen sitter alltså centralt och arbetar med hela koncernen och inte endast i Företag 2. Där arbetar de med att se hur arbetet går till på företaget, så att processerna går till som de ska och data används på ett regelrätt sätt. En konsult har även tagits in som är ansvarig för projektet inom verksamheten på Företag 2, som sedan rapporterar till den övergripande styrgruppen. Målet är att bli klara med arbetet och att processer och applikationer är regelrätta i december 2017. Förändringarna som skett och kommer ske inom företaget är inte många enligt respondenten. Respondent B menar på att de idag redan har höga krav på hantering av personuppgifter att de inte blir så stora skillnader med införandet av GDPR. Frågan om hur de skulle hantera

privatpersoners förfrågan att bli borttagna kunde respondenten inte svara på. Projektgruppen som arbetar med dataskyddsförordningen skulle höra av sig tre veckor efter intervjuns genomförande för att ge en uppdatering på åtgärder. Efter det skulle beslut tas i företagets ledningsgrupp för att besluta vart ansvaret skall komma att ligga. De största konsekvenserna för Företag 2 spås bli om kunderna vill hämta ut all information som registrerats om dem i applikationer och infrastruktur. Det beskriver respondenten som besvärligt men även som något alla företag kommer att få problem med. Inga nya roller är planerade att tillsättas, respondenten beskriver istället att mer arbete kommer att behöva läggas ned på arbetet kring GDPR. Han berättar som sagt att de inte kommer anställa några nya utan säkerheten kring hantering av kundernas data kommer stärkas med den befintliga arbetsstyrkan. Han beskriver deras nya säkerhetstänk som:

> *Istället för att titta på 100% kommer vi titta på 120%* - Respondent B

Den allmänna inställningen till införandet av GDPR är både positiv och negativ. Den ökade säkerheten över personuppgifter ses som en positiv förändring. Utan GDPR och tidigare relaterade lagar och deras krav på skydd av personuppgifter ser respondenten att företag inte helt säkert sett det som en prioritet att skydda. Respondenten framstod som säker på att de kommer bli i enlighet med GDPR.

## 4.3. Företag 3

### 4.3.1. Bakgrund

Företag 3 är en av Europas ledande modekedjor med över 480 butiker. De har butiker i elva länder, varav deras huvudmarknader är Sverige, Norge och Finland. De har även franchisebutiker i åtta länder, och en e-handelsbutik. Som kund kan du bli medlem i deras kundklubb. Medlemmarnas köp registreras och lagras, de data som lagras används bland annat till bonusberäkning. De använder Analytisk CRM och köphistoriken för att analysera köpmönster i allmänhet, exempelvis jämför de kunders köp i vanlig butik kontra online. Vilka är generella analyser och görs inte på individnivå.

Respondent C är projektledare på IT-avdelningen hos Företag 3. Hen har jobbat med projektledning av systemdesign där i drygt 20 år. Förra året fick respondenten uppdraget att undersöka GDPR och vad det innebär för företaget, samt vad som måste göras för att bli kompatibla med den nya dataskyddsförordningen.

### 4.3.2. Arbetet kring dataskyddsförordningen

A Senvåren 2016 startade Företag 3 ett analysprojekt. Den första anledningen till projektet var att studera den nya dataskyddsförordningen, för att få en bättre förståelse för den. Den andra anledningen var att dokumentera nuläget, exempelvis vilka behandlingar av persondata de har idag. De var ett team där respondenten var projektledare, och teamet bestod av anställda från IT-avdelningen, HR-avdelningen och marknadsavdelningen. När teamet var inlästa på dataskyddsförordningen och nuläget så gjorde de en Gap-analys. Gap-analys är ett affärsverktyg som gör det möjligt för ett företag att jämföra sin aktuella prestation med sin potentiella prestation. Med hjälp av analysen kunde de se vad de behövde adressera och vad som krävs för

att de ska bli kompatibla med dataskyddsförordningen. Resultatet av analysen blev en åtgärdslista, som de nu arbetar med att implementera.

Respondent C tror att mycket bra kommer att komma ut från den nya dataskyddsförordningen. Redan existerande data kommer kontrolleras då periodiska granskningar och behandlingar kommer genomföras. Företag 3 kommer utbilda och informera anställda, med fokus på de som jobbar med persondata. Ett mer strukturerat arbete kring persondataskydd ses som en trolig konsekvens av dataskyddsförordningen. Bland annat genom mera uppmärksamhet på de aktuella frågorna, samt en större medvetenhet.

> *Jag ser väl att konsekvensen är att vi förhoppningsvis blir bättre än vad vi är idag på informationssäkerhet och säkerhet vad gäller persondata.* - Respondent C

Kvalitén på säkerhetsarbetet beror idag på den anställde, då det är dålig struktur över hur arbetet ska gå till. Men med nya etablerade styrningsprocesser så får de anställda ledning och stöd, vilket Respondent C vet kommer bidra till mera struktur. Respondenten nämner även ökad dokumentation som en konsekvens av den nya dataskyddsförordningen. Processer och riktlinjer som ska förklaras och liknande för att få en tydlighet i arbetet. När det kommer till att informera kunderna så kommer uppdateringar kring hur kundernas personuppgifter hanteras göras på deras hemsida. Processer för utdrag av data och radering berättar respondenten att de redan har befintliga processer för. Det blir därför ingenting de behöver förändra i systemen. Företaget har idag personuppgifter i ostrukturerade data främst i deras ärendehanteringssystem. Respondenten nämner att de nu kommer behöva vara försiktigare med vad som skrivs där.

Inställningen till dataskyddsförordningen är endast positiv enligt Respondent C. Sanktionsavgifterna ses mer som en skrämseltaktik och ett sätt att poängtera hur viktigt det nya regelverket är från EU:s sida, och oroar därför inte hen. Respondenten anser att mycket i lagstiftningen handlar om att företagen ska veta vad de gör, med hjälp av tydliga riktlinjer och processer. Hen tror att företaget kommer bli bättre än vad de är idag på informationssäkerhet och säkerhet vad gäller persondata. De har börjat i god tid och ligger i fas, och har därför goda förhoppningar att få det gjort i tid.

## 4.4. Företag 4

### 4.4.1. Bakgrund

Företag 4 är en ledande aktör inom detaljhandeln i Sverige idag med cirka 1300 butiker runt om i landet. Butikerna drivs av enskilda aktörer som äger och driver sin butik. Företag 4 är en del av samma större koncern som Företag 2, vilket påverkar deras jobb med den nya dataskyddsförordningen på samma sätt som för Företag 2. Företag 4 har ett medlemskort som kunderna kan ansöka om att få. Utifrån det kortet samlar Företag 4 in information om kunderna. Det är alltifrån namn och personnummer till köp de gör. Kundernas privata information används sedan till företagets lojalitetsprogram så att de får riktade erbjudanden och bonuspoäng. Den här typ av kundhantering kan klassas som Analytisk CRM.

Respondent D har två roller på Företag 4, informationssäkerhetschef och personuppgiftsombud. Arbetet går ut på att styra, utveckla och kontrollera informationssäkerheten på företaget. Hens uppgift är även att svara på frågor som kommer från andra chefer inom verksamheten.

### 4.4.2. Arbetet kring dataskyddsförordningen

Arbetet kring dataskyddsförordningen på Företag 4 går till så att de har en projektgrupp på ett tiotal personer där en del jobbar som projektledare och andra som experter inom olika områden. De har även tagit externt juridiskt stöd för tolkning av den nya dataskyddsförordningen. Det positiva med externa arbetare är att de även jobbar gentemot flera kunder. Därför kan de få se arbetet från olika perspektiv, de är även bättre uppdaterade på domar ute i Europa. Det har varit viktigt med den juridiska hjälpen då Datainspektionen inte har så många resurser att diskutera frågor med. Det har lett till att de varit tvungna att göra många avväganden och bedömningar själva. Projektgruppen arbetar med att strukturera upp frågor kring GDPR. Det sker genom workshops och möten där det diskuteras hur de ska arbeta med de frågorna. Då Företag 4 ingår i en koncern har de även ett större program på central nivå som arbetar med GDPR. De har ett dataskyddsombud per affärsområde som samarbetar och ordnar möten där de kan diskutera frågor som uppstått. Företagets arbete kring GDPR har pågått sedan början av 2016 då de började arbeta med GDPR ostrukturerat. Innan årsskiftet började de sedan arbeta mer strukturerat med regelverket.

Respondenten har svårt att ange några konsekvenser och förändringar som kommer genomföras på Företag 4. Det beror på att en Gap-analys precis genomförts och åtgärder som kommer behöva genomföras utgår från den analysen. Resultatet av analysen kommer inte att vara klart förrän i juni. Men respondenten berättar att alla medarbetare kommer påverkas då de måste utbildas för att få nödvändig kunskap, processer blir påverkade och alla system måste bli i enlighet med GDPR. Lite mer konkreta exempel på vad som kommer förändras är att kundvillkoren kommer att behöva uppdateras, processer för incidenthantering kommer behöva sättas upp, funktioner för dataportabilitet måste tas fram där bland annat vilket format utlämnandet av data ska vara. Vilket format de ska använda vid utlämnandet ser respondenten som ett problem då det inte är definierat i lagtexten. Blir utlämnandet av information till privatpersoner uppmärksammat i Sverige eller utomlands kan det öka förfrågningarna påpekar respondenten. Beroende på vilket stöd och uppmärksamhet respektive ansvarig myndighet i medlemsländerna ger så kan förfrågningarna öka markant.

> *Det är en sån åtgärd som kan leda fram till att vi kan få, hypotetiskt kanske 1000 förfrågningar på folk som vill ha uppgifter från oss. Då måste vi självklart kunna ha en förmåga att kunna leverera...* - Respondent D

Den största konsekvensen för Företag 4 blir att alla IT-system måste genomgå förändringar och det är ett stort arbete i sig. Det kommer även krävas mer resurser i form av anställda. Bättre dokumentation nämns av respondenten som något positiv då det ger en slags spårbarhet i alla beslut och överväganden som görs. Hen beskriver även det, tillsammans med den nya sanktionsregeln, som en motivation till att göra allting rätt. En konsekvens som gäller för alla företag tror respondenten kommer handla om hur Datainspektionens arbete kommer utveckla sig. Om de kommer genomföra inspektioner eller om det kommer vara mer händelsestyrt, respondenten tror mer på det senare alternativet.

Inställningen till den nya dataskyddsförordningen var positiv och respondenten uttrycker ingen oro kring att inte hinna klart i tid med förberedelserna inför dataskyddsförordningen. Något respondenten nämner som ett problem med regelverket är att förstå hur hanteringen av ostrukturerade data ska gå till och hur de ska gå tillväga angående den delen. Den delen av dataskyddsförordningen beskrivs som luddig. Att förstå olika begrepp som nämns i dataskydds-förordningen anses vara svårt då det går att tolka dem på olika sätt.

## 4.5. Sammanställning av intervjuer

Mycket material framställdes av intervjuerna och för att få en klarare bild över vilka likheter samt vad som skiljer företagen åt presenteras nedan i tabell 3 en sammanfattning.

| | **Företag 1** | **Företag 2** | **Företag 3** | **Företag 4** |
|---|---|---|---|---|
| **Förändringar** | Förändra formulär för medlemskap<br>Ändring av många program<br>Bättre och säkrare processer<br>Anställa fler<br>Nya medgivanden från kunder | Inga specifika förändringar<br>Ej bestämt åtgärder<br>Om kunderna vill hämta ut registrerade personuppgifter<br>Inga nya anställda | Mer dokumentation<br>Uppdatera kundvillkor<br>Periodisk granskning av existerande data<br>Utbildning till anställda<br>Bättre styrningsprocesser för anställda<br>Mer struktur | Mer dokumentation<br>Uppdatera kundvillkor<br>Utbilda personal<br>Processer för incidenthantering<br>Kan bli en markant ökning av förfrågningar på personuppgifter<br>Anställa fler |
| **Inställning till införandet av GDPR** | Positivt inställd, arbetet flyter på bra<br>Frågetecken kring Artikel 29-gruppen och Datainspektionen<br>Inte oroliga, klara i tid | Ser inte så mycket förbättringar<br>GDPR gynnar privatpersoner och inte företag<br>Inte orolig över de kommande sanktionerna | Ser positivt på GDPR.<br>Anser att många bra saker kommer ut ur det.<br>Bra för både företag och kund.<br>Inte oroliga över att hinna klart i tid | Positiv inställning<br>Vissa ord saknar definition. Därför svårt att tolka.<br>Positiv till införandet av sanktioner<br>Uttrycker ingen oro över att hinna klart |

Tabell 3 - Sammanställning av studiens resultat

# 5. Analys

I det här kapitlet presenteras en analys på resultatet av studien. Kapitlet inleds med en jämförelse mellan företagen där de olika kraven från kravmodellen diskuteras. Därefter analyseras de olika konsekvenserna som företagen ser att GDPR ger för dem. Kapitlet avslutas med en presentation av kravmodellen det redogörs för vilka företag som arbetar med respektive krav.

## 5.1. Jämförelse mellan företagen

De två första punkterna som kravmodellen tog upp var rätten till rättelse och rätten till radering. Endast Företag 1 nämnde rätten till rättelse som en konsekvens av dataskyddsförordningen. Rätten till radering är en av de större förändringarna. Det med anledning av att PuL endast erbjöd radering av personuppgifter som erhållit en felaktig behandling, vilket inte kommer vara ett krav nu. Rosengren (2017) beskriver i sin artikel att det kan bli problem vid införandet av processer som ska hantera radering av personuppgifter då vissa IT-system kan behöva byggas om helt och hållet. Företag 1 nämner att det är ett stort arbete med att införa processer för att kunna hantera radering av personuppgifter, men är det enda företaget som gör det. Företag 3 nämner att de redan har processer för att hantera radering och utdrag av personuppgifter. De två andra företagen nämner varken rättelse eller radering vid intervjuerna som något de behöver förändra i sina system för att uppfylla GDPR:s krav.

Det var endast ett företag som nämnde att det infört rollen som dataskyddsombud, vilket kan ha berott på att den rollen ersätter en redan existerande roll. Då två av företagen ingår i samma koncern kan det utgås från att Företag 2 har ett dataskyddsombud, då respondenten i intervjun med Företag 4 nämnde att alla affärsområden inom koncernen har ett dataskyddsombud. Som tidigare nämnts i teorin så hade personuppgiftsombud inga formella krav, utan endast allmänna krav på tillräckliga kvalifikationer. Europaparlamentet och rådets förordning 2016/679 beskriver även att om en systematisk övervakning sker är det krav på att tillsätta ett dataskyddsombud. Hälften av de intervjuade företagen lever alltså inte upp till det kravet.

Kravmodellen nämner kravet på konsekvensbedömning, som ska ske i samband med varje ny personuppgiftsbehandling för att minimera riskerna. Konsekvensbedömningen ska genomföras för att se vilka risker behandling av personuppgifter medför. Inget av företagen nämnde att de genomfört en ny konsekvensbedömning eller att de planerat att genomföra en, trots att det kommer innebära mer arbete. Inget av företagen lever alltså upp till det kravet, vilket är det enda kravet inget av företagen har nämnt under intervjuerna av alla krav som GDPR innebär för dem.

Kravmodellen i avsnitt *3.3.2. Kravmodell* nämner att företagen kommer att behöva öka sin dokumentation över hur personuppgifterna behandlas är en viktig förändring som kommer med GDPR. Två av företagen, Företag 3 och Företag 4, tar upp det och är medvetna om den förändringen. Företag 3 nämner även att de behöver bli bättre på att informera hur behandlingen sker, vilket är en av anledningarna till att GDPR leder till ökad dokumentation (Martin Brinnen 2017).

Alla intervjuade företag har idag till viss del data om kunder i ostrukturerad form, såsom i mail. Det innebär att de idag använder sig av missbruksregeln, som är nästa punkt i kravmodellen. Det

medför extra arbete vid införandet av dataskyddsförordningen, då den typen av behandling av personuppgifter blir otillåten. Missbruksregeln är, som tidigare nämnts, en undantagsregel som företag och organisationer rekommenderas att inte använda. Därför har de som inte använder den en stor fördel vid borttagandet av missbruksregeln. Alla företag visade sig dock använda sig av den här regeln. Ett av företagen berättade att de skulle ta fram dokument för bland annat hur mailkommunikation med kunder ska utföras för att inte gå emot de nya kraven. Inget av företagen gav några rent konkreta och utförliga svar på hur det skulle gå till.

Gemensamt företagen emellan är att alla nämnde framtida problem med kunder som begär ut sina uppgifter eller vill bli raderade, vilket nämns i tabell 2 som en av de förändringar som behöver genomföras. Kunderna kan begära ut data från företagen och det är det som går under dataportabilitet. Företag 4 nämnde att det var svårt att definiera i vilket format som kundernas data ska lämnas ut i då lagen endast beskriver "*i strukturerat, allmänt använt och maskinläsbart format...*" (Europaparlamentets och rådets förordning 2016/679, Artikel 20, punkt 1). De andra företagen har inte nämnt några definitionsproblem utan beskriver en oro kring hur många kunder som kommer höra av sig. Respondent C nämnde inte dataportabilitet alls som en förändring Företag 3 skulle behöva införa, vilket kan tyda på att det inte ses som en större förändring hos dem. Det motsäger vad de andra företagen sagt och kravmodellen (tabell 2) i *3.3.2. Kravmodell*, dataportabilitet ett nytt krav som ställs på dem. Därför bör det ha nämnts i intervjun som en förändring som Företag 3 kommer att behöva genomföra. I avsnittet *3.2. GDPR:s skillnader från PuL*, nämndes Artikel 29-gruppen och att de har tagit fram exempel på vad dataportabilitet kommer att kunna användas till. Här används låtlistor som något kunderna kan begära ut. Det betyder att kunderna i praktiken skulle kunna begära ut köphistorik då vissa av företagen sparar sådan data. Även om företagen inte varit så ingående i hur dataportabilitet kommer påverka dem så har den här punkten i GDPR varit det som oroat mest. Inget av företagen vet hur det kommer utveckla sig, om många kunder kommer höra av sig eller om det inte uppmärksammas alls. Företag 4 nämnde att beroende på om det uppmärksammas mycket runt om i världen så kan kunderna bli mer medvetna om sina rättigheter och förfrågningarna kan komma att öka drastiskt. Respondent A på Företag 1 nämnde att dataportabilitet troligen inte kommer bli något problem för företag inom detaljhandeln.

Att uppdatera sina kundvillkor och samla in nya samtycken är ytterligare två krav som finns i kravmodellen (tabell 2) nämner. Av företagen var det två som nämnde de punkterna som en konsekvens av GDPR. Två av fyra företag nämner alltså inte nya samtycken och uppdatering av sina kundvillkor, trots att det troligen kommer kräva många resurser. Datainspektionen nämnde det i intervjun som något som alla företag behöver granska.

Som den sista punkten i kravmodellen nämner så kommer organisationer få en skyldighet att anmäla intrång inom 72 timmar, samt ett ansvar att i vissa fall kontakta de berörda personernas vars personuppgifter drabbats av intrånget. Skyldigheten medför högre krav på organisationen vid intrång än tidigare. Endast ett av företagen nämner nya processer för incidenthantering.

Alla företagen var medvetna om att många processer och program i företagens system var i behov av förändringar och granskningar, med undantag från Företag 2, för att överensstämma med lagen. Alla såg positivt på att behöva göra en granskning av alla systemen då det ger dem chansen till att strukturera upp alla data. Där stämmer Datainspektionen och företagens syn på

förändringar som kommer att behöva genomföras överens. Anledningen till varför Företag 2 inte tror att de kommer behöva genomföra så många förändringar beror på att de idag har mycket höga krav på hur de hanterar personuppgifter. De tror därför att de inte behöver förändra så mycket inom företaget. Datainspektionen talar om att även om företag har bra hantering av data idag så kommer ändå en genomgång av alla processer behöva en genomgång.

## 5.2. Företagen och Kravmodellen

Nedan i tabell 3 visas en sammanfattning från föregående avsnitt av vilka företag som lever upp till vilka krav utifrån kravmodellen som presenterades i avsnittet *3.3.2. Kravmodell.* De företag som nämner att de kommer genomföra förändringar för att leva upp till kraven som presenterades i kravmodellen markeras med ett "X".

| Nya krav | Förklaring | Företagen 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Rätten till rättelse | Företagens medlemmar ska ha rätt att få tillgång till sina personuppgifter samt kunna rätta dessa och kunna komplettera ofullständiga personuppgifter. | X | | | |
| Rätten till radering | Företagens medlemmar har nu "rätten att bli bortglömd", vilket betyder att företagen måste radera alla data kopplade till medlemmen. | X | | X | |
| Tillsätta ett dataskydds-ombud | Det nya dataskyddsombudet ersätter det tidigare personuppgiftsombudet från PuL. Dataskyddsombudet får fler krav att leva upp till. Undantag för företag med färre än 250 anställda som inte genomför systematisk övervakning. | | X | | X |
| Konsekvens-bedömning | genomföra en konsekvensbedömning för varje personuppgiftsbehandling som innebär risker för dem som behandlingen berör, samt se vad som kan göras för att minimera riskerna. | | | | |
| Dokumentations-krav | En ökad dokumentation kommer behöva ske i företagen. De måste börja dokumentera hur personuppgifterna behandlas. | | | X | X |
| Missbruksregeln | Personuppgifter som finns i ostrukturerat material som email måste tas bort. Det betyder att processer för hur personuppgifter hanteras i exempelvis supporten hos företagen måste ses över. | X | | X | X |
| Dataportabilitet | skapa processer för att kunna hantera kunder som vill flytta över sina personuppgifter till ett annat företag. | X | X | | X |
| Uppdaterade kundvillkor | uppdatera sina kundvillkor så att dessa är lättlästa och så att kunden kan godkänna varje behandling för sig. För ett företag inom detaljhandeln innebär det att se över hur kunderna informeras om hur personuppgifterna behandlas. Vid varje ny behandling måste kundvillkoren uppdateras. | X | | X | X |
| Samla in nya samtycken | samla in nya samtycken till de nya uppdaterade kundvillkoren. | X | | | |
| Incident-rapporteringskrav | skapa processer för hur incidentrapportering ska gå till. Måste anmäla incident senast 72 timmar efter händelsen inträffat. | | | | X |

Tabell 4 - Sammanställning av företagens arbete med GDPR:s nya krav.

## 5.3. Företagens upplevelser kring GDPR

Nedan analyseras företagens arbete med GDPR, hur de upplever att arbetet med dataskydds-förordningen går, hur de ser på de kommande sanktionsavgifterna och om de tror att de kommer hinna klart i tid.

De flesta av företagen såg fördelar med GDPR, men ingen nämnde det positiva med att EU får ett gemensamt regelverk. Trots att majoriteten av företagen finns i andra EU-länder nämnde ingen av dem hur samarbetet länder emellan kan förenklas av dataskyddsförordningen. Det är en fördel som kan tyckas gynna alla de intervjuade företagen. Sanktionerna kommer exempelvis att appliceras enligt GDPR och bör därför bli mer enhetlig, som det inte i dagsläget är enligt Tankard (2016). Alltså bör det bli lika stränga sanktioner mot alla företag som bryter mot GDPR i de olika medlemsländerna.

Tre av de fyra företagen hade tagit hjälp av jurister vid arbetet med den nya dataskyddsförordningen. Anledningen till det var bland annat för att det är svårt att tolka lagtexter utan juridisk bakgrund. Det uppmärksammar även Eriksson och Goldkuhl (2015) där de bland annat beskriver lagar och förordningar som "*olämpligt formulerade*" samt "*oklar och föråldrad begreppsbildning*" (Eriksson & Goldkuhl 2015). Både Företag 1 och Företag 4 nämnde att de haft problem med att tolka lagtexten och med att definiera vissa begrepp. Datainspektionen är medvetna om att företagen har svårt med lagtolkningar i GDPR och att speciella oklarheter har uppstått angående dataportabilitet. De upplever att många har problem med hur det ska tillämpas i företagen och att det inte finns någon klar definition på vilket format data ska lämnas ut i, vilket innebär problem.

En stor förändring som kommer med den nya dataskyddsförordningen är införandet av sanktionsavgifter. På grund av att det inte är något företagen förbereder sig för så ingår den förändringen inte i kravmodellen, men bör ändå analyseras. Sanktionsavgifterna kan uppgå till fyra procent av den globala omsättningen eller 20 miljoner euro, beroende på vilket värde som är högst, som nämns i kapitlel *3.2 GDPR:s skillnader från PuL*. Överlag var företagen inte oroliga över eventuella sanktionsavgifter. Ett av företagen såg sanktionsavgifterna som en skrämsel-taktik och ett sätt att poängtera hur viktigt det nya regelverket är från EU:s sida. Ett annat företagen nämnde att Datainspektionen troligen inte kommer ha resurser nog att kontrollera alla organisationer direkt när dataskyddsförordningen träder i kraft. Företaget trodde istället att det skulle bli händelsestyrt, vilket innebär att inspektionerna kommer att ske hos de som fått en anmälan eller liknande.

I intervjun med Datainspektionen nämner de att de flesta företagen kommer hinna klart med införandet i tid. Det stämmer bra överens med vad intervjuerna gav för svar. Inget av företagen var oroliga för att inte bli klara med anpassningen inför införandet 25:e maj 2018. Datainspektionen har endast haft kontakt med företag som aktivt sökt information kring den nya dataskyddsförordningen. Det kan betyda att det finns ett mörkertal på företag som inte kommit igång med arbetet kring dataskyddsförordningen och som då kanske inte kommer hinna klart i tid. I artikeln i det avslutande stycket i *3.2. GDPR:s skillnader från PuL* tror Finnegan (2017) att ungefär hälften av alla företag kommer hinna klart i tid. Rosengren (2017) är inne på samma spår och skriver om att inte alla kommer vara redo vid införandet 2018. Thornton (2017) är dock mer

samspelt med företagen och ser att de som följer det tidigare direktivet har en bra bas och behöver därför inte göra alltför många förändringar.

Inställningen till införandet av GDPR var mestadels positiv. Respondenterna ansåg att det var bra att privatpersoners rättigheter till sin egen personliga data styrktes och att företagen nu fick en direkt anledning att gå igenom och granska alla data. En av respondenterna hade en lite mer blandad syn på lagändringen, och kände tyngden av det arbete det innebär för att anpassa företaget till den nya dataskyddsförordningen. Hen ansåg nackdelarna vara fler än fördelarna ur ett företags perspektiv men påpekade att det var bra med ett förstärkt skydd för privatpersoner.

# 6. Slutsats och Diskussion

Det här kapitlet består av avsnittet slutsats där forskningsfrågorna som ställs i avsnittet *1.3 Syfte och forskningsfrågor* besvaras. Slutsats följs sedan av en diskussion kring studien, om den uppfyllt sitt syfte och samt en diskussion kring studiens begränsningar.

## 6.1. Slutsats

Syftet med den här studien var att se vilka förändringar företagen behöver göra för att uppnå GDPR:s krav, men även hur de arbetar med förordningen idag och hur de upplever att det går. En kravmodell skapades i kapitel *3.3.2. kravmodell* med de krav på som företagen behöver leva upp till för att inte begå lagbrott när GDPR införs. Utifrån den kravmodellen har sedan en analys genomförts och utifrån den kommer slutsatserna att dras. Studiens syfte anses ha uppnåtts, trots att svaren inte blev detsamma som förväntat då företagen ännu inte börjat arbeta med alla förändringar och kommande förändringar var ännu inte fullt klarlagda.

> 1. *Vilka förändringar anser företagen att de behöver genomföra och stämmer det överens med GDPR:s krav?*

kravmodellen som skapades i kapitel *3.3.2. kravmodell* redovisar alla krav som företagen måste uppfylla. Alla företagen förutom Företag 3 var överens om att dataportabilitet kommer påverka dem och att åtgärder kommer behöva ske för att kunna hantera den förändringen. Missbruksregeln samt uppdaterade kundvillkor nämnde alla företag utom Företag 2 som en förändring de skulle behöva göra inom företagen för att leva upp till de kommande kraven. Det var långt ifrån alla företag som nämnde att de behövde göra förändringar relaterade till alla kraven i kravmodellen. Det var inget av företagen som nämnde att de skulle behöva genomföra en konsekvensbedömning eller att de redan genomfört den. Ett av företagen stack ut från resten då de ansåg att få eller inga förändringar skulle behöva ske, vilket är ett ganska starkt antagande och talar emot vad de andra företagen uppfattat. Från kravmodellen kan slutsatsen dras att företagen arbetade med de olika kraven. Inget av företagen nämnde alla krav som något de arbetade med och inget av företagen nämnde konsekvensbedömning som något de skulle behöva genomföra eller redan hunnit genomföra på sina databehandlingar. Förändringarna de anser sig behöva genomföra på respektive företag stämmer därför inte överens med kraven som GDPR ställer på dem.

> 2. *Vilka konsekvenser upplever företagen att GDPR kommer få för dem och hur upplever de att arbetet med den går?*

Företagen var i en förberedande fas med arbetet kring GDPR och hade därför inte kommit så långt i arbetet kring den. De nämnde dock att fler anställda skulle behövas för att hantera kunder som hör av sig för att få sina uppgifter flyttade eller raderade. Det fjärde företaget, Företag 2, ansåg att de anställda som de har nu bör räcka som arbetsstyrka även efter att den nya dataskyddsförordningen trätt i kraft. Två av företagen nämner även utbildningar för anställda, och nya, mer strukturerade arbetssätt som arbetet kring GDPR kräver för att leva upp till kraven. Företagen såg positivt på att behöva genomföra en genomgång av alla system och dess data. De förklarade att det leder till en större medvetenhet kring vad det är för data som finns i systemen

samt vad det är de behandlar. De hade alla även en positiv syn till att hinna klart med arbetet kring förordningen innan 25 maj 2018. Sanktionsavgifterna var en av större förändringarna och Datainspektionen ansåg det vara en förändring som oroade många företag. Men utifrån intervjuerna med företagen så stämmer det inte, då de såg sanktionsavgifterna som en skrämseltaktik och som en motivation till att göra allt rätt. En förändring i och med införandet av GDPR som företagen såg mer problematiskt på var lagtolkning. Tre av företagen hade redan tagit hjälp av jurister. Två av företagen nämnde framtida anställningar som en konsekvens, och ett företag nämnde att de mer intensivt skulle granska alla kunddata. Det i sig innebär extra kostnader för företagen i form av personalkostnader på löneutlägg samt extra arbetstid som kan tillkomma vid ett utökat säkerhetsarbete. Anpassning till ett nytt regelverk innebär att starta projektgrupper som alla företagen nämner, att lägga ner tid på att gå igenom alla system och mer arbete i största allmänhet. Slutsatsen som kan dras från analysen är att företagen fortfarande är i ett tidigt stadie i införandet av dataskyddsförordningen och har därför inte kommit så långt i arbetet kring den. De har dock planerat utbildning av personal för att alla ska vara medvetna om de nya kraven och processerna som behöver införas. Företagen har även börjat sätta sig in i vad alla system gör, vad för data de behandlar och varför de behandlingarna genomförs, vilket alla upplever som en positiv effekt av GDPR. De får alla bättre koll på sina system och kan rensa bort sådant som inte bör finnas kvar. De upplever att de kommande sanktionsavgifterna finns till för att visa allvaret i den nya dataskyddsförordningen och hur viktigt det är att följa de nya kraven.

## 6.2. Diskussion

Beroende på om företagen haft en bra hantering av personuppgifter sedan tidigare så kan det avgöra om omställningen till GDPR:s regler kommer vara svår eller inte. En jämförelse av företag i olika EU-medlemsländer hade varit en intressant studie att genomföra och förmodligen gett ett annorlunda resultat. Det beror på, som tidigare nämnt, de olika nationella tolkningarna av det äldre direktivet. Därför hade det varit intressant att jämföra företag i olika länder istället för bara inom Sveriges gränser. Det hade även varit bättre att genomföra studien mer i slutskedet och precis innan 25:e maj 2018 när arbetet kring GDPR ska vara klart. Företagen hade då varit i slutstadiet av arbetet och därför haft en klarare bild av förändringar som regelverket inneburit för dem, och eventuella problem de upplevt.

Företag 2 stod ut från resten av företagen i studien då de ansåg att de inte skulle behöva genomföra så många förändringar för att leva upp till GDPR:s krav. Det kan bero på att de arbetar med receptbelagda mediciner och redan har bra ordning på all data de hanterar, vilket respondenten på företaget påstod. Det kan även vara så att det företaget inte var lika insatt i förberedelserna för GDPR och därför inte visste vilka förändringar de skulle behöva genomföra. Det företaget är en del av en större koncern och känner därför kanske inte samma ansvarskänsla som resterande företag gör då en del av arbetet ligger på central nivå. Det är även intressant att inte företagen ser potentialen i dataportabilitet då det är stor förändring och kan börja utnyttjas. Spellistan som kan begäras ut från Spotify skulle lika gärna kunna vara köphistorik från företagen. Respondent C nämnde inte dataportabilitet alls, vilket kan tyda på att det inte ses som en större förändring för Företag 3. Men det motsäger vad de andra företagen sagt och enligt GDPR är dataportabilitet ett nytt krav som ställs på dem. Därför bör det ha nämnts i intervjun som en förändring som Företag 3 kommer att behöva genomföra. Dataportabilitet kan förenkla

kundrelationshantering som nämns i kapitel *1.1.1. CRM* om kunden vill byta företag och då för över sina data till en konkurrent. Det kommer också bli viktigt att behandling av personuppgifter kommer göras enligt lag. Då dataportabilitet införs och företagen behandlar uppgifter som inte är tillåtna och de uppgifterna lämnas ut till en kund på begäran kan det skada företagets rykte. Därför kommer det vara viktigare för företagen att behandla personliga data rätt och enligt avtal som kunderna gett samtycke till.

Inget av företagen nämnde dataskyddsombud som en ny roll inom företagen. Eftersom att alla företagen använder CRM så kan det tolkas som att de genomför systematisk övervakning, vilket betyder att de måste införa ett dataskyddsombud. Även om alla de intervjuade företagen hade ett personuppgiftsombud sedan tidigare, är dataskyddsombud en roll värd att nämna som en konsekvens av lagen, då rollen kommer få en större betydelse för företaget. Inte bara för att det blir ett krav, utan även med tanke på de stora böter de riskerar att få om rollen inte tillsätts.

Endast ett av företagen nämnde incidentrapportering som en direkt förändring. Det kan betyda att det ses som en mindre prioriterad förändring. Inget av företagen nämnde konsekvensbedömning, vilket kan bero på att samtliga företag inte var klara med införandet. Det kan även tyda på att de ännu inte planerat att göra någon sådan eller så ansågs det inte som någon stor process värd att nämna. Både incidentrapportering och konsekvensbedömning är förändringar som handlar om framtida behandlingar. De inkluderar alltså inte ändringar på redan befintliga data, utan det är endast skillnader i hanteringar framöver. Även om det är två nedprioriterade förändringar bör de förberedas väl innan införandet av dataskyddsförordningen. Endast ett företag tar upp ökad dokumentation som en konsekvens av GDPR. Det kan vara för att företagen inte ser dokumentation som en stor förändring i förhållande till de andra punkterna, eller att den likt incidentrapportering och konsekvensbedömning inte känns aktuell innan dataskyddsförordningen träder i kraft.

Angående om företagen kommer hinna klart till införandet av GDPR den 25 maj 2018 så verkar företagen se positivt på det och anser sig hinna klart i tid. De verkade inte oroade över tidspressen. Enligt artikeln skriven av Finnegan (2017) i teorikapitlet kommer ungefär hälften av företagen inte vara färdiga med arbetet kring GDPR innan maj 2018, då slutdatum är satt. Det påståendet gäller företag ute i Europa också, vilket kan påverka siffrorna då det idag är olika lagar kring hantering av personuppgifter. Därför kan företag i vissa länder uppleva större problem och behöva mer förändringar vid införandet av GDPR. Men även i artikeln skriven av Rosengren (2017), har advokaten Frydlinger svårt att se att alla företag kommer vara fullt förberedda vid införandet. Det tidigare direktivet nämner Korff (2002) i en rapport att ett antal länder hade problem med att implementera direktivet 95/46/EG, liknande problem kan uppstå vid införandet av förordningen för de som i dagsläget inte har så bra personuppgiftshantering.

Studien anses att ha uppfyllt sitt syfte och svarat på de forskningsfrågor som ställts. Resultatet skulle kunna appliceras på företag inom detaljhandeln i Sverige som redan har en adekvat hantering av personuppgifter och därför inte står inför ett jättestort arbete kring GDPR. Den generaliseringen motiveras av att de företag som har en bra personuppgiftshantering liknar de företag som deltagit i studien. Studiens resultat är intressant ur ett IS-perspektiv då det påverkar alla företag och organisationer. IT-system påverkas av GDPR i hög grad då säkerheten måste ses över och bli bättre för att kunna leva upp till de nya kraven. Det är även intressant för människor

som arbetar med databehandling, att se hur företag har arbetat med förändringarna för att leva upp till kraven för att veta hur och vad de behöver göra.

### 6.2.1. Begränsningar

Valet att använda respondenter inom chefsroller kan ha påverkat resultatet. Chefer representerar inte alla som arbetar och kan ha en annan syn på arbetet gentemot vad de underordnade rollerna har. En annan påverkan kan vara att de med chefsrollen har en mer översiktlig syn på arbetet med dataskyddsförordningen som inte stämmer överens med exempelvis utvecklarnas syn på det. Det kan därför vara svårt att säga att en chef representerar ett helt företag, och därför kan resultatet blivit annorlunda om olika roller på företagen hade intervjuats. Utifrån svaren som gavs under intervjuerna var det mer övergripande svar som framställdes och inte djupgående, vilket hade varit att föredra. Fler respondenter inom varje företag hade varit ett bättre alternativ för att få en mer djupgående bild av hur hanteringen av den nya dataskyddsförordningen går till. Alla respondenter var inte aktiva i projektgruppen på respektive företag, vilket kan ha lett till mer ytlig intervju på grund av kunskapsbrist. Deltagande i projektgruppen som hanterar GDPR ger en större inblick i hur arbetet går till och kan därför ge en djupare kunskapsinsamling.

Svaren kan vara förädlade då företagen till en början inte var anonyma. Även respondentens inställning och persontyp kan ha påverkat bilden de förmedlat. Ser respondenten alla möjligheter och inga direkta hinder så kan en falsk känsla inges av att företaget ligger bra till med förberedelserna.

Urvalet kan även påverkats av att de företag som hade mycket kvar att göra var de som inte kunde ställa upp på intervju. Därför kan det slutgiltiga resultatet av intervjuer blivit representativt för de som hade bra personuppgiftshantering redan, och därför inte lika mycket att göra inför GDPR. Det kan vara anledningen till den likhet vi sett mellan intervjuerna. För studiens skull hade det varit mer intressant att intervjua företag som hade mera olika upplevelser av GDPR. Likhet mellan intervjuerna kan även grunda sig i att alla företag verkar inom detaljhandeln och deras arbetssätt liknar varandras mer än företag inom andra branscher.

## 6.3. Framtida forskning

Utifrån det resultatet som framställdes i den här studien skulle det vara intressant att se ytterligare studier på vilka konsekvenser och förändringar företagen faktiskt fick efter införandet av GDPR. Vad blev följderna av införandet, och blev förändringarna och konsekvenserna verkligen som företagen trodde? Mycket i den här studien är spekulationer och antaganden från företagens sida då de inte säkert kunde se några definitiva förändringar eller konsekvenser på grund av arbetet med dataskyddsförordningen inte var klar.

# Källförteckning

I källförteckningen skrivs inte företagens namn och hemsidor ut för att behålla företagens anonymitet.

## Intervjuer och personlig korrespondens

Brinnen, Martin. Uppsala/Stockholm, 2017-04-12, 2017-05-15
Respondent A, Uppsala/Insjön, 2017-04-18
Respondent B, Uppsala/Stockholm, 2017-05-04
Respondent C, Uppsala/Göteborg, 2017-04-28
Respondent D, Uppsala/Stockholm, 2017-05-12

## Källor


Article 29 data protection working party. (2016). *Guidelines on the right to data portability.* Bryssel: Europeiska kommissionen. Tillgänglig: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Barriball, K. L. (1994). Collecting data using a semi-structured interview: a discussion paper. *Journal of Advanced Nursing*, vol 19, ss. 328-335. Tillgänglig: https://www.researchgate.net/profile/Alison_While/publication/234055873_While_A_Collecting_data_using_a_semi-structured_interview_A_discussion_paper_Journal_of_Advanced_Nursing_192_328-335/links/0fcfd50ea96fa548fd000000.pdf [2017-05-04]

C5 Alliance (2017). *GDPR is not just a problem for your IT department*
Tillgänglig: https://www.c5alliance.com/latest/gdpr-not-just-problem-department/ [2017-05-15]

Chan, J. (2005). Toward a Unified View of Customer Relationship Management. *The Journal of American Academy of Business*. 25 Mars. Tillgänglig: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.575.3312&rep=rep1&type=pdf [2017-04-25]

Chen, I. J. & Popovich K. (2003). Understanding customer relationship management (CRM) People, process and technology. *Business Process Management Journal*, Vol. 9, ss. 672-688 Tillgänglig: http://cis.csuohio.edu/~ichen/CRM.pdf [2017-04-07]

Datainspektionen I (2017). *Förberedelser för personuppgiftsansvariga*
*Vägledning till personuppgiftsansvariga inför den nya dataskyddsförordningen 2018.*
Tillgänglig: http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/forberedelser-for-personuppgiftsansvariga/ [2017-01-29]

Datainspektionen II (2017). *Missbruksregeln försvinner*. Tillgänglig: http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-forsvinner/ [2017-02-13]

Datainspektionen III (2017). *Allmänna frågor*. Tillgänglig: http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/allmanna-fragor/ [2017-03-31]

Datainspektionen IV (2017). *Datainspektionen 1973-2011*. Tillgänglig: http://www.datainspektionen.se/om-oss/historik/ [2017-03-31]

Datainspektionen V (2017). *Om Datainspektionen*. Tillgänglig: http://www.datainspektionen.se/om-oss/ [2017-03-31]

Datainspektionen VI (2017). *Nyheter med dataskyddsförordningen*. Tillgänglig: http://www.datainspektionen.se/dataskyddsreformen/forberedelser/nyheter-med-dataskyddsforordningen/ [2017-04-06]

DiCicco-Bloom, B. & Crabtree, B. F. (2006). *The qualitative research interview Medical Education*, vol. 40 ss. 314-321

Dimond, R. (2015). *Analysing Semi-Structured Interviews: Understanding Family Experience of Rare Disease and Genetic Risk*. Tillgänglig: http://methods.sagepub.com.ezproxy.its.uu.se/dataset/semistructured-interviews-genetic-risk [2017-05-12]

Direktivet 95/46/EG. EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Eriksson, O. & Goldkuhl, G. (2015) *Studie av en samling offentliggemensamma digitala resurser: Informationsförsörjning för ekonomiskt bistånd.* Tillgänglig: http://www.vits.org/publikationer/dokument/794.pdf [2017-06-07]

EU-upplysningen (2016-05-24). *Olika typer av EU-lagar.* Tillgänglig: http://www.eu-upplysningen.se/Om-EU/Om-EUs-lagar-och-beslutsfattande/Olika-typer-av-EU-lagar/ [2017-05-22]

Europaparlamentets och rådets förordning 2016/679. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Europeiska Kommissionen I (2017). *Obligations of data controllers*. Tillgänglig: http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm [2017-04-14]

Europeiska Kommissionen II (2016) *Guidelines on the right to data portability* [Elektronisk] Rapport. Bryssel, Europakommissionen. Tillgänglig: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf [2017-05-15]

Finnegan, M. (2007). [Elektronisk] Cloud can help ease burden of GDPR compliance for businesses, Google execs claim. *Computer World UK*, 4 maj. Tillgänglig: https://www.computerworlduk.com/cloud-computing/cloud-can-help-ease-burden-of-gdpr-compliance-for-businesses-google-execs-claim-3658526/ [2017-05-13]

Fusch P. I. & Ness L. R. (2015). *Are We There Yet? Data Saturation in Qualitative Research.* Tillgänglig: http://tqr.nova.edu/wp-content/uploads/2015/09/fusch1.pdf [2017-02-14]

Gerring, J. (2006). *Case study research*. New York: Cambridge University Press.

Gutwirth, S., Leenes, R. & de Hert, P. (2015). *Reforming European Data Protection Law*. Vol 20. Brussel: Springer.

Internet live stats (2017) Tillgänglig: http://www.internetlivestats.com/internet-users/ [2017-05-08]

Iriana, R. & Buttle, F. (2006). Strategic, Operational, and Analytical Customer Relationship Management: Attributes and Measures. *Journal of Relationship Marketing*. Vol. 5 Issue 4.

Knox, S., Maklan, S., Payne, A., Peppard, J. & Ryals, L. (2003). *Customer Relationship Management - Perspectives from the Marketplace*. Burlington: Butterworth-Heinemann.
Kostojohn, S., Johnson, M. & Paulen, B. (2011). *CRM Fundamentals*. New York: APress.

Korff, D. (2002). EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE. *Comparative Summary of national laws*. Cambridge. Tillgänglig: http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE [2017-04-02]

Lagen.nu (2017). *Lagtolkning*. Tillgänglig: https://lagen.nu/begrepp/Lagtolkning [2017-06-07]

Langhorn, R. & Jaibaji, A. (2017). *The upside of GDPR: a potential remedy for your "dark" data*. Tillgänglig: https://www.ibm.com/blogs/think/nl-en/2017/03/20/upside-gdpr-potential-remedy-dark-data/ [2017-06-07]

Oates, B. J. (2006). *Researching Information Systems and Computing London*. SAGE Publications Ltd. 2005.

Privacyline (2017). *Ny lagstiftning 2016/2018 - DATASKYDDSFÖRORDNINGEN.* Tillgänglig: http://www.privacyline.se/web/page.aspx?refid=175 [2017-01-31]

Rosengren, L. (2017). *Juristen: ”Det är hög tid att börja med GDPR-arbetet”.* Tillgänglig: http://cio.idg.se/2.1782/1.681447/juristen-gdpr [2017-05-02]

SFS 1998:204. Personuppgiftslag.

Sturges J. E. & Hanrahan K. J. (2004). Comparing telephone and face-to-face qualitative interviewing: a research note. *Qualitative Research 4*, vol. 4, ss. 107-118. Tillgänglig: http://journals.sagepub.com.ezproxy.its.uu.se/doi/pdf/10.1177/1468794104041110 [2017-04-27]

Tankard, C. (2016). *“What the GDPR means for businesses”*. Network Security. Tillgänglig: http://ac.els-cdn.com.ezproxy.its.uu.se/S1353485816300563/1-s2.0-S1353485816300563-main.pdf?_tid=5b0be564-1dd5-11e7-9d01-00000aacb361&acdnat=1491818965_8cdd74c22867d367b402a91df03ad2e4 http://digpath.co.uk/wp-content/uploads/NESE_2016-06_Jun.pdf [2017-04-02]

Tsiptis, K. & Chorianopoulos, A. (2009). *Data Mining Techniques in CRM: Inside Customer Segmentation* [Elektronisk] Chichester: John Wiley & Sons, Ltd. Tillgänglig: https://pdfs.semanticscholar.org/e4ca/f946c219d9afd433dcad02679ba346e8d5ce.pdf [2017-02-06]

Walsham G. (1995) *The Emergence of Interpretivism in IS research* [Elektronisk] Catonsville: The Institute for Operations Research and the Management Sciences, Tillgänglig: http://gkmc.utah.edu/7910F/papers/ISR%20emergence%20of%20interpretivism%20in%20IS%20research.pdf [2017-02-06]

Williams, D. S. (2014). *Connected CRM: Implementing a Data-Driven, Customer-Centric Business Strategy*. Hoboken: John Wiley & Sons
Williamson, K. & Bow, A. (2002). *Research methods for students, academics and professionals: information management and systems*. Wagga Wagga: Elsevier Science

# Bilagor

## Bilaga 1

**Frågor till datainspektionen:**

1. Är det många företag inom dagligvaruhandeln som hör av sig till er (nu)?
    a. Om ja: vad är det de frågar/undrar över?
2. Upplever ni att företagen är medvetna om vilka förändringar som behöver ske?
    a. På vilket sätt?
3. "Räknar" ni med att de flesta företag kommer hinna klart i tid?
    a. Om nej: Varför inte, och vad händer då?
4. Hur hjälper ni företagen nu innan införskaffandet av GDPR?
5. Vad är de största problemen ni ser att företagen står inför?
    a. Hur löser man dessa?
6. Upplever ni att företagen ser positivt eller negativt på ändringen?
    a. Varför?
7. Vilka konsekvenser ser ni att företagen kommer få?
    a. Ser ni några negativa konsekvenser som kommer ut ur detta?

**Kompletterande frågor:**

1. Finns det någonting du tror är lätt för företagen att missa när dom arbetar med införandet av den nya dataskyddsförordningen?
    a. Om ja: Vad och varför?
2. Vilka är de största förändringarna du tror företagen kommer behöva göra?
3. Om ett företag idag har bra hantering av personuppgifter, tror ni att de ändå behöver genomgå många förändringar?
    a. Förklara varför/ varför inte.
4. Hur ställer sig företag i frågan om dataportabilitet?
    a. Många som hör av sig om det?
    b. Ser dom mycket problem med det?

## Bilaga 2

- Berätta om dig och din roll på företaget.
- Hur många jobbar med införandet av GDPR? (vilka? Vad gör dom?)
- Vilka förändringar kommer ni att göra innan införandet av GDPR?
- Vilka konsekvenser tror ni att införandet av GDPR kommer ge? (lista med möjliga konsekvenser, kunna fiska, “har ni tänkt på…?”)
- Hur kommer ni att påverkas av dessa konsekvenser/ändringar?
- Vad för bra/dåligt kommer komma ut från detta? (varför)
- Har ni idag personuppgifter i ostrukturerade data?
- Hur kommer ni hantera privatpersoner som hör av sig och vill veta hur deras personliga data hanteras/ vill bli borttagna?