YRKESHÖGSKOLAN
NOVIA

GDPR-förordningens påverkan på bokföringsbyråerna i Finland

En kvalitativ undersökning av hur GDPR-förordningen har påverkat bokföringsbyråerna, samt vad de gjort för att anpassa sig till det nya regelverket

Mathias Broman

Examensarbete för Tradenom (YH)-examen

Utbildningsprogrammet i Företagsekonomi

Åbo 07.03.2019

Examensarbete

Författare: Mathias Broman

Utbildning och ort: Företagsekonomi, Åbo

Inriktningsalternativ/Fördjupning: Redovisning

Handledare: Marika Nygårdas

Titel: GDPR-förordningen påverkan på bokföringsbyråerna i Finland - En kvalitativ undersökning av hur GDPR-förordningen har påverkat bokföringsbyråerna, samt vad de gjort för att anpassa sig

---

Datum 07.03.2019 Sidantal 30 Bilagor 1

Abstrakt

Regelverket togs i bruk den 25 maj 2018. Den nya förordningen togs i bruk eftersom EU inte längre kunde garantera sina medborgares rättigheter i dagens digitalt expanderande värld. GDPR kommer med nya bestämmelser över hur personuppgifter skall behandlas. Det spelar ingen roll var i världen personuppgifter behandlas, så länge det är frågan om en EU-medborgare skall behandlingen ske i enighet med GDPR. Ett företag som inte följer GDPR kan få förödande bestraffning.

Inom bokföringsbranschen behandlas det en stor mängd personuppgifter. De företag som även sköter lönehantering och HR-tjänster behandlar dessutom en hel del känsliga personuppgifter. Detta innebär att bokföringsbyråerna i samband med GDPR måste se till att deras arbetsrutiner inte på något sätt går mot GDPR.

Syftet med examensarbetet är att ta reda på hur bokföringsbyråerna har påverkats av GDPR, samt vad de har gjort för att anpassa sig till förordningen. Företagen har haft en lång tid att förbereda sig för GDPR, och därmed kommer det att undersökas vilka konkreta åtgärder bokföringsbyråerna har tagit till och hur deras arbete har förändrats.

Undersökningen har gjorts genom att sammankoppla teori och kvalitativ forskning. Två personer med olika positioner i två olika företag har intervjuats. Teorin kretsar främst kring det officiella GDPR-dokumentet, men också kring intern kontroll och säkerhet.

Resultatet visar att det inte nödvändigtvis har skett så stora förändringar i arbetet, men att arbetsrutinerna inom företaget har blivit säkrare för företaget och dess kunder. En av de största förändringarna i arbetsrutinerna är att man undviker användning av e-posten och använder sig istället av säkrare plattformar för informationsbyte mellan tjänsteleverantör och kund.

Språk: Svenska Nyckelord: GDPR, bokföring, personuppgifter

BACHELOR'S THESIS

Author: Mathias Broman
Degree Program: Business Administration
Specialization: Accounting
Supervisor(s): Marika Nygårdas

Title: The GDPR Regulation's Effect on Accounting Companies in Finland- A Qualitative research about the Effect of the GDPR Regulation on Accounting Companies, and What They Have Done to Adapt

---

Date 01.02.2019 Number of pages 30 Appendices 1

Abstract

GDPR was taken into force on 25 May 2018. The regulation was introduced as a result of the fact that the European Union no longer could guarantee their citizens' rights in today's digitally expanding world. GDPR introduces new standards of how personal data should be processed. The GDPR regulation affects every company or organization that processes personal data of citizens of the EU. It does not matter if the processing is taking place outside of the EU as long as personal data of EU citizens is being processed. A company that does not comply with the regulation may be devastatingly punished. In the field of accounting personal data processing occurs frequently. The companies that also offer payroll accounting and HR-services may process a lot of sensitive personal data. As a result of the regulation the companies in the field of accounting have to make sure that their processing of personal data complies with the GDPR.

The purpose of this Bachelors' thesis is to find out how accounting companies have been affected by GDPR, and what they have done to adapt to the regulation. The companies have had plenty of time to prepare for the adaption of the regulation, and the concrete measures are being examined in this Bachelors' thesis.

The examination has been done through linkage of theories and a qualitative research model. Two persons with different positions at two different companies have been interviewed. The theories grasp the official GDPR regulation, and in addition theories about internal control and security.

The result of this Bachelor's thesis indicates that the changes that have come with the regulation have not been too drastic, but the processing within the company has taken a more secure approach. One of the most notable changes is that companies try to avoid the processing of personal data through e-mail. As an alternative, platforms with increased security is being used for processing personal data.

Language: Swedish Key words: GDPR, Accounting, Personal data

Innehållsförteckning

1 Inledning

Under flera års tid har det diskuterats inom EU om hur man skall skydda sina medborgare och deras personuppgifter inom dagens digitala värld. EU:s dataskyddsdirektiv från 1995 blir allt mer föråldrat och blir för varje år som går mera irrelevant. Sättet som vi idag behandlar personuppgifter på har på grund av över 20 år av digital utveckling ändrat totalt, vilket betyder att man inte längre kan garantera sina medborgares säkerhet. Som ett resultat av detta togs GDPR-förordningen i bruk den 25 maj 2018. GDPR påverkar alla företag och organisationer som på ett eller annat sätt behandlar EU-medborgares personuppgifter.

I det här arbetet kommer jag att behandla hur GDPR-förordningen har påverkat bokföringsbyråernas verksamhet. En bokföringsbyrå behandlar ofta stora mängder personuppgifter och GDPR ställer höga krav på hur det skall göras på ett säkert sätt. Det är därför viktigt att se över sina rutiner och hur uppgifterna behandlas. Även hur alla personuppgifter lagras måste ses över. Ett företag eller en organisation som bryter mot någon av punkterna i förordningen kan få allvarliga straff. Ett företag kan bestraffas med böter på en summa ända upp till 4 % av företagets globala omsättning.

Jag valde det här ämnet eftersom det har påverkat mitt arbete och jag fick då intresse för det. Jag började jobba på en bokföringsbyrå i samband med att GDPR togs i bruk. Själv fick jag ta del av mycket information om hur arbetet skall skötas i fortsättningen, men jag valde att gå in på det på ett djupare plan i samband med det här arbetet.

1.1 Frågeställning

Den genomgående frågeställningen jag har i mitt arbete är att ta reda på hur bokföringsbyråerna har påverkats av GDPR. GDPR ställer höga krav på säkerhet, men lämnar ganska mycket att tolka. Det står inte i förordningen exakt hur ett företag skall göra, utan det handlar snarare om att företag måste kunna motivera varför de behandlar personuppgifter och hur de gör det med säkerheten i åtanke.

1.2 Syfte och mål

Målet med mitt arbete är att ta reda på vad bokföringsbyråerna har gjort för att anpassa sig till GDPR. Jag vill ta reda på vilka konkreta åtgärder och vilka nya arbetsprocesser som tagits i bruk i samband med förordningen. Eftersom jag själv är anställd på en bokföringsbyrå är jag intresserad av att veta på ett djupare plan hur det har påverkat

branschen. Jag har själv fått ta del av den delen som påverkar personalen, men målet med det här arbetet är att få en djupare inblick i hur det har påverkat och vad bokföringsbyråerna har gjort för att följa GDPR.

1.3 Avgränsning

Jag kommer i mitt arbete att avgränsa mig till stora bokföringsbyråer inom Finland. Med stora bokföringsbyråer anser jag de största aktörerna i Finland, med flera hundra anställda. I de företag som är stora i Finland men som även är verksamma i andra länder kommer jag enbart att fokusera på arbetet i Finland. Situationen kan se annorlunda ut i mindre företag och bland näringsidkare, men det kommer inte att tas upp i detta arbete.

2 GDPR

EU:s dataskyddsdirektiv från 1995 innehöll redan mycket av det som nu är aktuellt med GDPR. På den tiden som direktivet gjordes skedde lagring av personuppgifter på ett helt annat sätt än i dagens digitalt expanderande värld. Därför krävdes det en modernisering av direktivet som uppdaterar bestämmelserna och lägger ett större ansvar på alla aktörer som behandlar personuppgifter. (eugdpr, u.d.)

General Data Protection Regulation, förkortat GDPR, trädde i kraft den 25 maj 2018. GDPR är en ny förordning inom EU, som strävar till att skydda alla sina medborgare inom dagens digitala värld. Även om GDPR bygger på många gamla direktiv, introduceras också nya bestämmelser som påverkar företag såväl som privatpersoner. Förordningen, som introducerades av EU-kommissionen den 25 januari 2012, röstades igenom av europaparlamentet den 14 april 2016. (eugdpr, u.d.)

GDPR är en förordning och är en uppdatering och modernisering av EU:s dataskyddsdirektiv 95/46/EG. Det finns en stor skillnad mellan ett direktiv och en förordning. Ett EU-direktiv sätter upp mål för medlemsländerna som de sedan själva bestämmer hur de skall nå. En förordning däremot, är en bindande rättsakt. Alla länder måste i sin helhet tillämpa en förordning. (europa, 2018)

Den största skillnaden jämfört med tidigare direktiv, är att GDPR gäller alla företag som behandlar personuppgifter av personer bosatta inom EU. Detta innebär alltså att ett företag som är lokaliserat utanför Europa, men behandlar EU-medborgares personuppgifter, berörs av den nya förordningen. Ett företag som inte följer direktiven kan bötfällas. Det maximala

straffet är den större summan av antingen 4 % av företagets globala årliga omsättning, eller 20 miljoner euro. (eugdpr, u.d.)

GDPR handlar till stor del om en EU-medborgares rätt till sin egen personliga data. Data som eventuellt kan knytas till en person, exempelvis adress, telefonnummer och IP-adress, bör lagras på ett säkert sätt. En privatperson skall också ha rätten att få tillbaks sina data om den så önskar när den slutar köpa tjänster från ett företag. Detta leder i sin tur till svåra tolkningar eftersom GDPR kan hamna i strid med andra lagar. En bokföringsbyrå behandlar en enorm mängd personuppgifter både av sina kunder samt deras kunders kunder. Om någon i kedjan önskar få tillbaks sina personuppgifter kan det leda till problem. Detta eftersom det finns andra lagar och bestämmelser över exempelvis hur länge en bokföringsbyrå måste spara allt till bokföringen hörande material. Ett annat exempel på detta är Facebook, som tidigare inte lät sina användare radera sina profiler, utan endast inaktivera dem. I samband med GDPR måste det ske ändringar så att en användare har rätt att få tillbaka alla sina personuppgifter, förutsatt att det inte strider mot andra lagar. (Investopedia, 2019)

2.1 Personuppgifter

Det är viktigt att definiera vad som är personuppgifter, eftersom GDPR endast innefattar den sortens data. Enligt GDPR definieras en personuppgift som ”en upplysning som avser en identifierad eller identifierbar fysisk person”. En identifierbar fysisk person definieras som ”en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”. Enligt GDPR:s definitioner innebär det alltså att förordningen bör följas av alla de företag och organisationer som på något sätt utför en behandling av uppgifter som kan knytas till en fysisk person. En fysisk person är en helt vanlig människa. En juridisk person omfattas alltså inte av GDPR. Exempel på en juridisk person kan vara en förening, ett företag eller ett dödsbo. (GDPR, 2016, p. 111)

Det är ändå svårt att avgöra vad som exakt räknas som en personuppgift. Ett telefonnummer eller en adress kan ofta användas för att identifiera en person, medan ett vanligt namn eller en IP-adress inte nödvändigtvis anses vara personuppgifter. (GDPR, 2016, p. 111)

Det finns två kategorier för personuppgifter, normala och speciella. Normala kategorin innefattar bl.a. telefonnummer och adress. Speciella kategorin innefattar bland annat:

- brottsregister, exempelvis fällande domar i brottsmål.

- biometrisk data, dvs ”personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter”. (GDPR, 2016, p. 113)

- genetiska uppgifter, dvs ”alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga”. (GDPR, 2016, p. 113)

- uppgifter om hälsa, dvs ”personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus”. (GDPR, 2016, p. 114)

Detta innebär alltså att den speciella kategorin till en stor del handlar om personuppgifter som är extra känsliga. Det kan vara mycket skadligt att personuppgifter som telefonnummer och adress hamnar i fel händer. Generellt kan det ändå anses att personuppgifter i den speciella kategorin är ännu skadligare om de behandlas felaktigt. Det rör sig om mycket privata uppgifter och i fel händer kan det leda till exempelvis allvarlig diskriminering. (Westerlund, 2018, pp. 51-56)

Information om en person, oberoende av kategori, behöver ändå inte nödvändigtvis falla under GDPR-förordningen. Personuppgifter räknas som personlig data endast då den används för att identifiera en fysisk person. Detta betyder alltså att data, i en ostrukturerad form som inte behandlas, inte faller under GDPR. (Westerlund, 2018, pp. 51-56)

Figur 1 – Visualisering av exempel på vanliga och känsliga personuppgifter

(Samlogic, u.d.)

2.1.1 Behandling av personuppgifter

Som tidigare nämnt räknas uppgifter som personuppgifter endast då de behandlas för att identifiera en fysisk person. Detta innebär alltså att data i sin rena form inte nödvändigtvis bör falla under GDPR, även om det i data finns uppgifter om personer (Westerlund, 2018, p. 55). GDPR definierar behandling som

> en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. (GDPR, 2016, p. 111).

Allt det som beskrivs i förordningen som behandling faller under GDPR. Det blir därmed svårt att avgöra ett fall behandling av personuppgifter inte skulle falla under GDPR. Ett exempel på när detta kan ske är när en person läser data som är ostrukturerad och inte läses med intentionen att identifiera en fysisk person. Det är svårt att ha en klar gränsdragning och det lämnar med andra ord mycket att tolka och motivera för de som avgör ifall en behandling som inte skulle falla under GDPR skulle ske. (GDPR, 2016, p. 111)

Profilering är en del av behandling. Profilering av personuppgifter är då de används för att bedöma personliga egenskaper hos en fysisk person. Detta används främst för att analysera eller förutsäga exempelvis en fysisk persons arbetsprestation, ekonomiska situation eller personliga preferenser. (GDPR, 2016, p. 111)

Pseudonymisering är även ett centralt begrepp som används. GDPR definierar det som

> en behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Det är med andra ord en säkerhetsåtgärd som kan användas vid behandling av personuppgifter (GDPR, 2016, p. 112)

2.1.2 Personuppgiftsansvarig och personuppgiftsbiträde

En personuppgiftsansvarig definieras enligt GDPR som ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt”. (GDPR, 2016, p. 112)

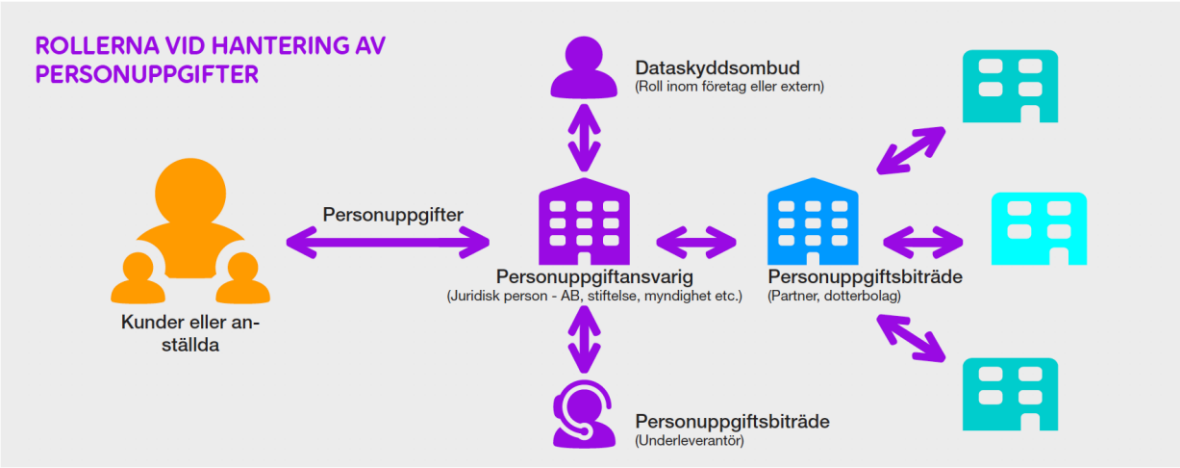
Ett företag eller organisation som fastställer ändamål och medel är alltså personuppgiftsansvarig. Det betyder att om företaget eller organisationen bestämmer varför personuppgifter behandlas och hur de skall behandlas, faller det inom ramen för regelverket. Ett företag eller en organisation kan också vara gemensamt personuppgiftsansvarig. Gemensamt personuppgiftsansvarig innebär att två eller flera företag/organisationer bestämmer varför och hur personuppgifter behandlas. I detta fall måste ett avtal ingås där parternas ansvar för att följa reglerna i förordningen fastställs. (europa, u.d.)

Ett exempel på gemensamt personuppgiftsansvarig är då ett företag erbjuder en tjänst via sin hemsida, men ett annat företag erbjuder någon form av tilläggstjänst i samband med det. Det kan röra sig om ett företag som säljer produkter men själva inte erbjuder hemtransport. Om de i sin tur har ett annat företag som via sin hemsida för en tilläggskostnad erbjuder hemkörning av produkten, och de tillsammans tillhandahåller hemsidan, är företagen gemensamt personuppgiftsansvariga. (GDPR, 2016, p. 53)

En personuppgiftsansvarig är skyldig till att inom 72 timmar anmäla till tillsynsmyndigheten ifall det sker en personuppgiftsincident. Om anmälan inte lämnas in inom 72 timmar krävs det en motivering på varför fördröjningen har skett. En personuppgiftsincident innebär att en fysisk person riskerar fysisk, materiell eller immateriell skada, exempelvis förlust av kontrollen över de egna personuppgifterna. (GDPR, 2016, p. 53)

Ett personuppgiftsbiträde definieras av GDPR som *en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.* (GDPR, 2016, p. 112)

Ett personuppgiftsbiträde är ofta en tredje part utanför företaget som behandlar en personuppgifter på en personuppgiftsansvarigs vägnar. Ett personuppgiftsbiträde kan exempelvis vara ett lönehanteringsföretag som sköter utbetalning av löner och andra relaterade löneuppgifter för ett annat företag. Det betyder att företaget som anlitat lönehanteringsföretaget fastställer varför och hur personuppgifterna behandlas och är därmed personuppgiftsansvarig. Lönehanteringsföretaget som hanterar personuppgifterna på personuppgiftsansvariges vägnar är på så vis personuppgiftsbiträde i detta fall. (europa, u.d.)



Figur 2 - Rollerna vid hantering av personuppgifter (www.cygate.se, 2017)

2.2 De registrerades rättigheter

I samband med GDPR-förordningen har rättigheterna för de vars personuppgifter behandlas stärkts. Ägaren till personuppgifterna ska ha rätt till information angående när och hur deras personuppgifter behandlas. De ska även ha kontroll över sina uppgifter. Den personuppgiftsansvarige är skyldig till att meddela den registrerade när uppgifter samlas in. (Datainspektionen, u.d.)

Information angående behandlingen skall kunna ges ut till den registrerade kostnadsfritt, lättillgängligt samt skrivet på tydligt och enkelt språk. (Datainspektionen, u.d.)

Med GDPR kommer även rätten till rättelse. Om en personuppgiftsansvarig har felaktiga eller utdaterade uppgifter har den registrerade rätten att få uppgifterna rättade. Det gäller också komplettering av saknade uppgifter som är relevanta för ändamålet. Den registrerade har även rätt att be om radering av uppgifter. Det är inte alltid så lätt att uppgifterna bara kan raderas. Man kan inte bara gå till polismyndigheten och be om att få sitt brottsregister raderat. Radering gäller i de fall då exempelvis uppgifterna inte längre behövs. Man har även rätt att återkalla det samtycke man har gett. För att företag inte ska göra fel listar datainspektionen några tips som är bra att följa. Personuppgifter skall endast lämnas ut till rätt person. Om det sker komplettering, redigering eller radering av personuppgifterna så måste den registrerade identifieras. Hur identifiering skall ske finns inte skrivet i GDPR, utan företaget måste själv besluta hur det görs. De skriver också att man aldrig skall samla in uppgifter i onödan. Detta kan bli knepigt eftersom man i samband med identifiering kan vara tvungen att behandla fler personuppgifter. Om den registrerade anser att den personuppgiftsansvarige har agerat på ett sätt som strider mot förordningen, kan ett klagomål lämnas in. Om den registrerade anses ha goda grunder för sitt klagomål, kan den ha rätt till skadestånd. Skadeståndet skall i regel ersätta för hela skadan som den personuppgiftsansvarige har gjort sig skyldig till. (Datainspektionen, u.d.)

3 GDPR inom bokföringsbranschen

För ett företag inom bokföringsbranschen leder GDPR till nya utmaningar. En bokföringsbyrå behandlar ofta en oerhört stor mängd personuppgifter. Det är inte bara sina egna kunders personuppgifter man behandlar, utan även kundernas kunders personuppgifter. Detta gör att bokföringsbyråer måste vara mycket noga med GDPR och dess bestämmelser. De måste ha ett säkert sätt att lagra all den information man besitter. De måste även fundera på vilka kommunikationskanaler och plattformar de använder för att utbyta information med sina kunder. För de bokföringsbyråer som även sköter lönehantering betyder det stora förändringar, eftersom man behandlar mycket personuppgifter. Där måste rutiner som exempelvis hur man skickar ut lönespecifikationer ses över.

Personuppgifter behandlas på flera olika ställen inom en bokföringsbyrås verksamhet. Eftersom all det till bokföring hörande materialet sparas och lagras sker behandlingen av personuppgifter mycket frekvent. Personuppgifter kan hittas i enskilda verifikat,

kundregister, leverantörsregister samt på fakturor. Det innebär ett stort ansvar för byråerna att se till att endast de personer som bör ha tillgång till uppgifterna har det. De bokföringsbyråer som även sköter lönehantering för andra företag behandlar även en hel del personuppgifter. Dessutom kan det röra sig om känsliga personuppgifter. Då måste man vara noga med att exempelvis arbetsrutinerna gällande lönespecifikationerna är säkra och inte hamnar i fel händer. Det krävs i enighet med GDPR ett säkert sätt att förflytta information som innehåller personuppgifter mellan sändare och mottagare. Då måste det göras beslut om vad man använder som huvudsaklig kommunikationskanal. Medan e-posten är lätt och smidig att använda finns det många säkerhetsrisker med den. Riskerna beskrivs mer noggrant senare i arbetet. Andra alternativ kan vara att ta i bruk säkra och krypterade molntjänster, som möjliggör ett lätt men också ett säkert sätt att utbyta information. På en bokföringsbyrå sker ett stort utfall av informationsbyte då exempelvis kunderna delar med sig av alla leverantörs- och kundfakturor. Då det beroende på leverantören och kunden finns stor risk för att fakturan innehåller personuppgifter, måste säkerheten ses över. Samma sak gäller på lönehanteringssidan då kunden till lönehanteringstjänsten måste dela med sig om en massa personuppgifter. (foretagarna.se, 2018)

3.1 Informationssäkerhet

Informationssäkerhet och lagring är en central del av GDPR. Bokföringsbyråer, som besitter en stor mängd personuppgifter, måste med noggrant säkerhetstänk fundera över hur personuppgifter behandlas och lagras. Den information som lagras skall inte få läcka ut, förvanskas eller förstöras. Det är också viktigt att se till att endast de personer som faktiskt behöver informationen har tillgång till den. De kunder som uppger sina personuppgifter skall också ha rätt till att veta hur och varför deras personuppgifter behandlas. Kärnan i GDPR är att skydda personers integritet och att värna allas friheter och rättigheter. (Datainspektionen, u.d.)

Vad vart och ett företag måste göra för att följa förordningen är till stor del upp till dem själva. GDPR ger riktlinjer men lämnar ganska mycket att tolka. Det är företagets eller organisationens ansvar att se till att säkerhetsarbeten uppfyller kraven i GDPR. Datainspektionen listar fyra punkter som är viktiga. Företaget eller organisationen måste se till att de:

- följer alla de grundläggande principerna i dataskyddsförordningen
- har en korrekt rättslig grund för sina personuppgiftsbehandlingar
- dokumenterar hur de har tänkt och hur de gör
- har struktur, rutiner och förutsägbarhet i sitt informationssäkerhetsarbete

(Datainspektionen, u.d.)

Till de grundläggande principerna hör man måste kunna svara på varför personuppgifter behandlas och vad ändamålet är. Det är också viktigt att ta reda på vilken rättslig grund som stöder behandlingen av uppgifterna. Dokumentation är en av nycklarna till GDPR. Förordningen ställer höga krav på dokumentation så det är väldigt viktigt att se över sina rutiner. (Datainspektionen, u.d.)

Nedan listas några av de grundläggande principerna i dataskyddsförordningen. Ett företag eller en organisation måste se till att de

- har stöd i GDPR för att behandla personuppgifterna
- endast samlar in de personuppgifter som behövs för ändamålet
- endast behandlar de personuppgifter som behövs för att uppnå ändamålet
- kontrollera personuppgifternas riktighet
- raderar personuppgifterna när de ej mera anses vara behövliga
- skyddar personuppgifterna på ett sånt vis att ingen obehörig har tillgång till dem
- kan motivera och bevisa hur de följer dataskyddsförordningen

(Datainspektionen, u.d.)

Som bekant lägger detta ett stort ansvar på den personuppgiftsansvarige. Det är upp till den personuppgiftsansvarige att själv se till att behandlingen sker i enighet mer förordningen, samt kunna motivera varför och hur saker och ting sker. (Datainspektionen, u.d.)

3.2 Laglig behandling av personuppgifter

I det officiella GDPR-dokumentet listas sex stycken villkor på laglig behandling av personuppgifter. Behandling av personuppgifter är endast laglig om åtminstone ett av följande villkor uppfylls:

1. ”Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål”

2. ”Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.”

3. ”Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.”

4. ”Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.”

5. ”Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.”

6. ”Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.”

(GDPR, 2016, pp. 118-119)

Intressant att notera är att samtycke endast är ett av de sex kraven. Det vill säga att om det inte finns möjlighet till att få samtycke finns det fem andra möjligheter att lagligt få behandla personuppgifter.

3.3 Villkor för samtycke

GDPR ställer en del krav på hur ett villkor för samtycke skall se ut. Den personuppgiftsansvarige är skyldig till att kunna visa att behandling av personuppgifterna har samtyckts av den registrerade. Om exempelvis samtyckesdelen är inkluderat i ett mera ingående avtal, måste delen med samtycke klart och tydligt kunna urskiljas. GDPR ställer också krav på att ett redigt språk måste användas. Den som har lämnas sitt samtycke skall

när som helst ha rätt att återkalla det. Grundprincipen är att återkallande av samtycke skall vara lika lätt som att ge det. Den registrerade bör informeras om detta. (GDPR, 2016, p. 122)

Om den registrerade inte är myndig kan andra regler gälla. För att ingå ett samtyckesavtal direkt med den registrerade måste den vara åtminstone 16 år. Medlemsstaterna har i sin tur rätt att sänka åldern, men inte lägre än 13 år. Om den registrerade är under den bestämda åldern, måste samtycke godkännas av den som har föräldraansvar för barnet. (GDPR, 2016, p. 123)

4 Intern kontroll

För att GDPR skall kunna följas krävs det klar intern styrning och kontroll. Intern kontroll är i grund och botten ordning och reda. Det handlar om de åtgärder som ett företag tar till för att öka den interna säkerheten, nå sina mål och minimera risker. Åtgärder som företag kan ta sig till kan handla om exempelvis klara arbetsprocesser, rutiner och inbyggda kontroller. Det finns otaliga mängder exempel på företagskatastrofer i historien som kunde ha undvikits eller åtminstone minimerats med rät intern kontroll och styrning. Det kan ha att göra med att anställda inte fått en klar beskrivning av hur saker och ting skall skötas som leder till misstag. Det kan också handla om situationer då tvåhandsprincipen inte har använts och en person har haft för stora rättigheter utan kontroll av flera personer, exempelvis då det kommer till utbetalningar. Den interna kontrollen lägger även stor vikt på riskbedömning. Det är väldigt viktigt som företag att vara medveten om vilka risker som finns och hur man hanterar dem. Riskhantering behandlas senare i kapitlet. (Wikland, 2014)

För att följa GDPR krävs det ett klart och redigt system. Det är mycket viktigt att endast de som faktiskt behöver personuppgifter har tillgång till dem. De behöver också lagras på ett säkert sätt vilket är en central del av den interna kontrollen. Det är viktigt för företag som behandlar personuppgifter att se över hur uppgifterna behandlas och lagras. (Datainspektionen, u.d.)

4.1 Register över behandling

Vid behandling av personuppgifter krävs det av den personuppgiftsansvariga och personuppgiftsbiträdet att skriftligt föra register över behandlingen. Registret skall vara tillgängligt i elektroniskt format och hållas uppdaterat. I det officiella GDPR-dokumentet nämns för personuppgiftsansvariga följande sju punkter. Registret skall innehålla:

- namn och kontaktuppgifter för den personuppgiftsansvarige
- ändamålen med behandlingen
- en beskrivning av kategorierna av registrerade och av kategorin personuppgifter
- de kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnat ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
- i tillämpliga fall, överföringar av personuppgifter till tredjeland eller en internationell organisation
- om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter
- om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna (GDPR, 2016, p. 158)

För personuppgiftsbiträden är registret minde krävande. I förordningen nämns följande fyra punkter som registret bör innehålla:

- namn och kontaktuppgifter för personuppgiftsbiträdet
- de kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.
- i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder. (GDPR, 2016, p. 159)

Huvudregeln är att endast företag med över 250 anställda bör föra register. Ett företag eller en organisation måste föra register oberoende av storlek om behandlingen är annat än tillfällig, sannolikt medför risker för de registrerades rättigheter eller friheter eller omfattar känsliga personuppgifter. (Datainspektionen, u.d.)

4.2 Risker

Det finns många risker då det kommer till behandling och lagring. Uppgifterna måste behandlas i enighet med GDPR-förordningen och lagras på ett säkert sätt. Personuppgifterna

skall vara tillgängliga endast för dem som har behov av att behandla dem. Därför är det viktigt att fundera på riskerna som finns och vad man kan göra åt dem.

Det finns fyra olika sätt att handskas med en risk, eliminering, reducering, delning med andra eller acceptering. Med eliminering avses det att man helt och håller gör sig av med en risk. Det kan vara svårt i praktiken och kräva mycket resurser. Ett exempel på detta kan vara att en bokföringsbyrå som ger alla sina anställda tillgångar till all lagrad information. För att eliminera risken att fel information hamnar i fel händer kan man göra så att endast de som behöver den specifika informationen har tillgång till den. En risk kan också reduceras. Risken finns alltid att plattformen man använder för informationslagring och utbyte kan hackas. För att reducera risken kan man använda en så säker plattform som möjligt med extra säkerhetsåtgärder. Att dela risken med andra innebär ofta att man skaffar en försäkring. Man kan också acceptera en risk. Det innebär att man är välmedveten om risken, men anser att det finns andra viktigare saker, samt att man är beredd att ta konsekvenserna. I bilden nedan kan man bekanta sig närmare med de olika sätten som kan användas för att hantera risker. (Wikland, 2014, p. 35)

Figur 3 - Olika sätt som används för att hantera risker (ssrma, u.d.)

Det är viktigt för företag och organisationer att har rutiner för att upptäcka och utreda personuppgiftsincidenter. En personuppgiftsincident innebär att någon förlorar kontrollen över sina uppgifter deras rättigheter och friheter riskeras. Det kan röra sig om att många personuppgifter har läckt ut och de drabbade riskeras av diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust eller brott mot sekretess eller

tystnadsplikt. Om personuppgifter har blivit förstörda, gått förlorade eller kommit i orätta händer handlar det också om en personuppgiftsincident. (Datainspektionen, u.d.)

Om det sker en personuppgiftsincident är företaget skyldigt till att anmäla det. GDPR slår fast att en incident bör anmälas inom 72 timmar. Om en incident inte anmäls kan företaget eller organisationen straffas med sanktionsavgifter på upp till 10 miljoner euro eller 2% av den globala omsättningen. (Datainspektionen, u.d.)

Om företaget inte har lämnat in en anmälan inom 72 timmar krävs det en motivering för förseningen. Ett personuppgiftsbiträde är skyldigt till att utan dröjsmål meddela en personuppgiftsansvarig när man fått information om att en personuppgiftsincident har skett. En anmälan om en personuppgiftsincident måste åtminstone innehålla fyra följande punkter:

- En beskrivning av personuppfitsincidentens art. I beskrivningen skall det ingå en uppskattning av det ungefärliga antalet registrerade samt antalet personuppgiftsposter som berörs.

- Namn på uppgifterna på kontaktuppgifterna för dataskyddsombudet.

- En beskrivning av sannolika konsekvenser av personuppgiftsincidenten.

- En beskrivning på de åtgärder som den personuppgiftsansvarige har tagit sig till för att åtgärda incidenten. Den skall också gärna innehålla åtgärder som kan användas för att milda skadan som är gjord. (GDPR, 2016, p. 162)

Dessutom finns det bestämmelser angående rapportering till den registrerade vars personuppgifter har varit med om en personuppgiftsincident. Den registrerade skall utan onödigt dröjsmål informeras om att en incident har skett ifall den utsätts för en hög risk. Den registrerade skall få information om personuppgiftsincidentens art genom en klar och tydlig beskrivning. Information om en personuppgifts incident behöver inte meddelas till den registrerade ifall:

- ”den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.”

- ”den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.”

- ”Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.” (GDPR, 2016, pp. 163-164)

Om den personuppgiftsansvarige inte går under något av de tre ovanstående påståendena, och den registrerade ännu inte har informerats, kan tillsynsmyndigheten bedöma sannolikheten för att den registrerade är under hög risk i samband med incidenten. Om tillsynsmyndigheten anser att den registrerade är under hög risk, måste antingen personuppgiftsansvarige eller personuppgiftsbiträdet informera den registrerade eller se till att något av de tre ovanstående villkoren uppfylls. (GDPR, 2016, pp. 163-164)

4.3 Säkerhet vid behandling

Behandling av personuppgifter måste ha en hög säkerhetsnivå som är lämplig i förhållande till risken. Det finns flera olika metoder att använda sig av och två centrala begrepp som beskrivs i GDPR är pseudonymisering och kryptering av personuppgifter. Pseudonymisering, som tidigare definierats, är då uppgifter ställs upp på ett sätt som inte längre gör det möjligt tillskrivas en fysisk person. Detta innebär alltså att uppgifterna behandlas på ett sätt att det inte är möjligt att identifiera en registrerad. (GDPR, 2016, p. 112) Kryptering nämns också som en lämplig skyddsåtgärd. Kryptering innebär att data omvandlas så att endast den tänkta mottagaren av informationen har tillgång att använda den. Det handlas om elektronisk data som omvandlas till en annan form av data som försvårar det märkbart för ett utomstående att ta del av informationen. (Datainspektionen, u.d.)

Det skall gå att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemet. Detta för att ständigt hålla en hög säkerhetsnivå. GDPR nämner också att det skall gå att snabbt återställa tillgänglighet till personuppgifterna vid en fysisk eller teknisk incident. Regelbunden testning, undersökning och utvärdering av behandlingsystemen är även nödvändigt för att upprätthålla säkerheten. (GDPR, 2016, p. 161)

Riskerna måste tas i beaktande då man bedömer säkerhetsnivån. Risker inkluderar men är inte begränsat till ”oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.” (GDPR, 2016, p. 161). Det är den personuppgiftsansvariges skyldighet att se till att alla de som utför arbete för företaget eller organisationen endast behandlar personuppgifterna på det sätt som den personuppgiftsansvarige har instruerat arbetaren till att göra. (Datainspektionen, u.d.)

Figur 4 - Visualisering av säkerhet vid behandling (Sentor, u.d.)

4.4 Dataskyddsombud

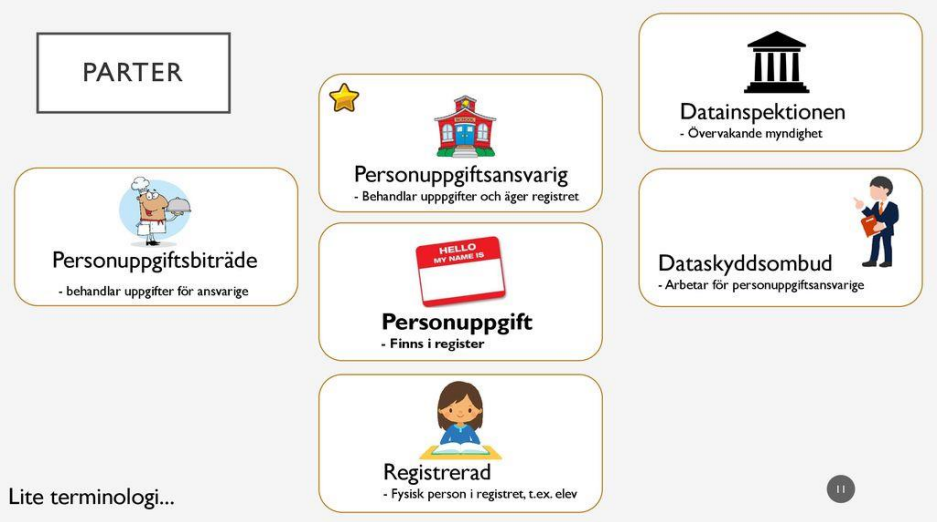
För att GDPR skall följas inom företag eller organisationer som behandlar personuppgifter bör de utse ett dataskyddsombud. Enligt GDPR skall en personuppgiftsansvarig eller ett personuppgiftsbiträde utnämna ett dataskyddsombud om:

- ”behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet”

- ”den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller”

- ”den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10”

Till dataskyddsombudets uppgifter hör att informera och ge råd till den personuppgiftsansvarige. De ska även övervaka att förordningen följs. Dataskyddsombudet fungerar lite som en brygga mellan personuppgiftsansvarige och tillsynsmyndigheten. (GDPR, 2016, pp. 170-172)



Figur 5 - Parter vid behandling av personuppgifter (Slideplayer, 2018)

4.5 Säkerhet för personuppgifter via e-post

Hur man använder sin e-post är viktigt att se över i samband med reformen. E-post är ett säkerhetsmässigt bristfälligt sätt att dela information, pga. de många riskerna som finns. Ett problem med e-post är att det är väldigt svårt att spåra mottagaren av informationen. Någon kan hacka in sig på en e-post utan att lämna speciellt klara spår. Dessutom går ett mejl sällan rakt från en sändare till en mottagare. Ett mejl passerar olika servrar som gör det möjligt för obehöriga att ta del av informationen. Dessutom utgör dagens moderna e-post funktioner en risk. Många plattformar har funktioner som automatiska listor och automatiska ifyllningar av adresser som gör att sändaren i misstag kan skicka mejlet fel. (Datainspektionen, u.d.)

Intern e-post anses allmänt vara säkrare, men det finns också felaktiga bilder av den. Man skulle kunna tro att intern e-post endast kan tillgås av de med rättigheter men det finns andra

faktorer som kan göra det osäkert. Ett exempel är om antivirus eller spamtvätt sköts av en extern leverantör. Även synkronisering med mobila enheter utgör en säkerhetsrisk eftersom de kan användas utanför företagets lokaler eller nätverk. (Datainspektionen, u.d.)

Det är upp till den personuppgiftsansvarige att säkerhetsställa behandlingen av personuppgifter i e-post. Ett personuppgiftsbiträde skall behandlas enligt den personuppgiftsansvariges instruktioner. En enskild anställd skall behandla uppgifter enligt sin arbetsgivares instruktioner och inte fatta egna beslut. (Datainspektionen, u.d.)

4.5.1 Riskbedömning

Om en personuppgiftsansvarig behandlar personuppgifter i sin e-post är det viktigt att det görs en riskbedömning. Det gäller då att ta till rätta säkerhetsåtgärder. Det kan då vara bra att se över riskbilden, hot, konsekvenserna samt åtgärder för att minska riskerna. Den personuppgiftsansvarige måste säkerhetsställa en lämplig risknivå i relation till vilken sorts samt vilken mängd personuppgifter som behandlas. Då det kommer till e-post är det väldigt svårt att undvika behandling av personuppgifter. I de flesta fall anses en e-postadress vara en personuppgift. Det som i meddelandet behandlas som kan kopplas till en person faller också under personuppgifter. Enligt förordningen krävs det också ett ännu starkare skydd ifall känsliga personuppgifter behandlas. Det beror på att känsliga personuppgifter utgör ett större hot mot en medborgares rättigheter. (Datainspektionen, u.d.)

Om känsliga personuppgifter behandlas måste den personuppgiftsansvarige se till att de behandlas på ett sätt som gör det omöjligt för obehöriga att ta del av uppgifterna. Då är det viktigt att meddelanden är krypterade. Medan många kommunikationsplattformer har någon form av ett inbyggt krypteringssystem gäller det också att ha särskilda krypteringsnycklar eller externa programvaror som krypterar alla meddelanden. (Datainspektionen, u.d.)

4.5.2 Arbetsrutiner

Den personuppgiftsansvarige ansvarar för att förordningen följs. Om personuppgifter behandlas måste det ske dokumentering som bevisar att behandlingen sker på ett säkert sätt i förhållande till förordningen samt att riskerna tas i beaktande. Hela den delen av personalen som har tillgång till personuppgifterna måste undervisas i sina arbetsrutiner så att ingenting blir felhanterat. Arbetsrutinerna vid inkommande epost med känsliga personuppgifter måste även ses över så att de behandlas på rätt sätt. (Datainspektionen, u.d.)

GDPR är ett omfattande regelverk som ställer höga krav på företag och organisationer som behandlar EU-medborgares personuppgifter. Teoridelen har kretsat till stor del kring GDPR, personuppgifter i bokföringen samt internkontroll och riskhantering.

5 Forskningsmetod

I det här kapitlet presenteras forskningsmetoden som använts för att samla in data. Med hjälp av boken företagsekonomiska metoder, (Bryman, 2013), har jag kunnat navigera genom de olika alternativen. Jag har i mitt examensarbete använt kvalitativ forskning i form av intervjuer, en strukturerad och en semistrukturerad. Jag valde kvalitativ forskning på grund av att jag på det sättet fick ett bättre underlag för mina forskningsfrågor.

5.1 Kvalitativ forskning

Kvalitativ forskning är en forskningsstrategi. Forskningen fokuserar då oftast mera på ord än kvantifiering när det kommer till insamling och analys av data. Kvalitativ forskning skiljer sig från kvantitativ forskning på det viset att den fokuserar på förståelse av den sociala verkligheten. Man vill i undersökningen komma åt hut deltagarna tolkar den. Kvalitativa intervjuer är ett vanligt sätt att använda inom kvalitativ forskning. De finns tre olika sorters intervjuformer som används:

- Strukturerad intervju, dvs en intervju där forskaren har alla frågor färdigt planerade. Forskaren är då oftast intresserad av sina egna intressen, istället för att den intervjuade öppnar upp sina egna uppfattningar om ämnet. Fördelen är då att det blir lättare att analysera svaren och få en högre validitet.

- Semistrukturerad intervju, dvs forskaren har en form av intervjuguide med sig, men är inte bunden till att exempelvis ställa frågorna i just den ordningen. Det öppnar också upp möjligheten för att ställa följdfrågor och ha ett friare samtal. Man kan då också öppna upp för en diskussion som gör det lättare att analysera den intervjuades verklighetsbild och uppfattning.

- Ostrukturerad intervju, dvs en intervju utan färdiga frågor. Forskaren kan ändå använda sig av exempelvis minnesanteckningar eller liknande. Det finns också den möjligheten att forskaren endast ställer en fråga och låter den intervjuade öppna upp på djupet inom ämnet.

> När det kommer till kvalitativ forskning rekommenderar författarna i boken att använda sig av semistrukturerade eller ostrukturerade intervjuer. Då kommer man bättre åt den intervjuades förståelse av den sociala verkligheten. (Bryman, 2013, pp. 390-401, 474-477)

5.2 Val av metod

För att få det bästa möjliga underlaget för min forskning valde jag att använda mig av intervjuer. Till intervjuerna valde jag att intervjua två personer med olika ställningar på två bokföringsbyråer som bäst speglar min avgränsning. Mitt mål var att använda mig av två semistrukturerade intervjuer med detaljfrågor om GDPR och dess påverkan. Dessvärre var en av intervjupersonerna mycket upptagen och föredrog att svara på frågorna via mejl. Jag försökte därför att utforma frågorna på ett sätt som gav mig detaljerade svar eftersom möjligheten att ställa tilläggsfrågor saknades.

5.3 Intervjuernas genomförande

Intervjuerna genomfördes med hjälp av nio frågor som handlade om GDPR och dess påverkan. Intervjupersonerna hade olika ställningar inom sina respektive företag vilket gav en bättre helhetsbild av situationen. Intervjupersonerna önskade förbli anonyma så jag kommer i fortsättningen hänvisa till person X som jobbar för företaget X, samt person Y som jobbar för företaget Y.

Person X är servicechef för kontoren i Västnyland på ett av de stora bokföringsföretagen i Finland. Person X har varit med och implementerat de krav som har satts av GDPR. Person X har på så sätt en bra bild av hur arbetet har påverkats med den nya förordningen. Jag intervjuade person X i ett slutet utrymme på dess anställdas kontor. Mina frågor ställdes i ordningsföljd, men det blev också en del följdfrågor för att öppna upp för diskussion. Intervjun varade i 35 minuter.

Person Y satt i sitt företag med i projektgruppen som ansvarade för att implementera bestämmelserna från GDPR-förordningen. Företaget är multinationellt och Person Y satt med i projektgruppen för Finland. Frågorna besvarades tillsammans med ett team där det ingick representanter från ekonomi-, löne- och HR-avdelningen samt styrelsen.

5.4 Analysmetod

Intervjun med Person X valde jag att banda in med min telefon. Jag gjorde det för att kunna transkribera svaren och göra det lättare att analysera dem. Eftersom intervjun var semistrukturerad valde jag att sedan se närmare på de delar av intervjun som mest var relevant i förhållande till mina forskningsfrågor. I intervjun med person X fick jag detaljerade och välformulerade svar per mejl. Jag valde här också att fokusera mest på den delen av svaren som var mest relevant för min forskning.

5.5 Tillförlitlighet

Det finns en mycket splittrad bild vad gäller reliabilitet och validitet inom kvalitativ forskning. Medan vissa anser att de fortfarande är lika relevanta som i kvantitativ forskning hävdar vissa forskare att reliabilitet och validitet inte uppnår samma relevans inom kvalitativ forskning. (Bryman, 2013, pp. 400-401)

Undersökningen kan anses vara tillförlitlig med tanke på de positioner de jag intervjuat har haft under den tid då GDPR-förordningen har implementerats. Målet med min undersökning var inte att få fram statistisk data utan snarare att få reda på de konkreta ändringar som medföljts av förordningen.

6 Undersökningens insamlade data

I det här kapitlet redogör jag för de svar jag fått av intervjupersonerna. Jag har valt att strukturera det på det viset att jag skriver ut frågorna och skriver om vad de båda intervjupersonernas svar.

Har det skett konkreta ändringar i ert arbete pga. GDPR?

Person X på hävdar att ändringarna inte har varit så stora på bokföringssidan, men att det har skett stora förändringar på lönesidan. De har i företag X gjort en sådan splittring, att man har en skild avdelning som räknar löner. Detta har gjorts för att ha bättre kontroll över vem som har tillgång till vilken information. Bokförarna har inte längre tillgång till de personuppgifter som endast används på lönesidan. Om en bokförare sedan i sin tur behöver någon av de uppgifter till bokslutet som endast löneräknarna har tillgång till, måste de be om den. Då har de en arbetsrutin där löneräknaren skalar bort personuppgifterna och delar endast med sig av siffrorna till bokföraren. De har även tagit i bruk nya kundportaler speciellt för deras största kunder. Detta har man gjort för att öka på säkerheten då man delar utför

informationsbyte mellan bokförare/löneräknare och kund. Kundportalen används ändå främst i lönehanteringens syfte. De har infört en policy gentemot sina kunder där de helst inte tar emot material via e-post från sina kunder. Person X nämner att de inte kan hindra kunder från att dela material via e-posten, men att de själv aldrig skickar personuppgifter till kunderna via deras e-post. En ny kundportal dit kunderna får egna inloggningsuppgifter är redan i användning och utveckling. Den används för att dela material med varandra på ett säkert sätt. Inom den interna e-posten som är säkrare kan det röra sig personuppgifter, men Person X säger att man arbetar för att minimera det.

Person Y berättar om att förberedelserna började redan i ett tidigt skede. Inom projektgruppen jobbade de i det tidiga skedet mest med att se över företagets plattformar och system. En stor del av deras fokus var att se över hur GDPR påverkar arbetsrutinerna inom företagets system. Det var ett mycket omfattade arbete att få i kraft ändringarna till den 25 maj 2018 då förordningen togs i bruk. Person Y nämner ändå att det handlar om ett genomgående arbete som inte slutade där. De har gått över från projektfas till ett pågående arbete. Just nu ligger deras fokus på att ta till fortsatta åtgärder, kartläggning av långsiktiga risker och planering av deras riskhantering.

Har GDPR medfört fördelar till ert arbete?

Person X säger att arbetet främst har blivit svårare. Vissa arbetsprocesser har blivit längre eftersom all information inte mera är lika lättillgänglig. Person X nämner det att man nu skilt måste be om information när man inte själv har tillgång till den som ett konkret exempel. Som fördelar listar Person X bland annat det att man minskat på användningen av E-posten för att ge plats för mera säkra plattformar för informationsbyte. Person X betonar vikten i att kunden kan känna sig säker med hur saker och ting sköts.

Person Y berättar att de nya systemen och arbetsprocesserna har gjort allting säkrare. Eftersom företaget behandlar en massa personuppgifter på bokföringssidan och en hel del känsliga personuppgifter på lönehanterings- och HR-avdelningen har det gjorts ett omfattande arbete så att rutinerna är i enighet med GDPR. Person Y nämner att deras behandling av personuppgifter redan före förordningen till stor del överensstämde med GDPR. Tack vare det omfattande arbetet har man kunnat identifiera risker och göra förändringar enligt dem. Det omfattande arbetet har även lett till förändringar till större helheter utöver dataskyddet. Kartläggningsarbetet har lett till utvecklingsmål på flera olika områden. En stor fördel som Person Y listar är de nya avtalen som skrivs mellan kund och

tjänsteleverantör. Det är i både företagets och kundens bästa intresse at det görs överenskommelser när det kommet till dataprocessernas säkerhet.

Har GDPR medfört nackdelar?

Som nackdelar listar person X främst de förändringar som har skett i arbetsrutinerna. Förändringar kan ofta anses vara jobbiga. Med tanke på hur lätt e-posten var att använda var det också en stor förändring att istället använda andra plattformar. De undviker även helt och hållet att skicka ut lönespecifikationer via epost. För att göra det krävs det ett skriftligt godkännande av personen i fråga. Som alternativ använder de antingen nätlöner eller löner till pappers.

Person Y berättar att de kortsiktigt har uppstått en hel del extra kostnader. Det har varit ett omfattande arbete att se till att alla processer följer GDPR, vilket har varit mycket tidskrävande. En annan komplikation har varit det att GDPR lämnar mycket att tolka och att de ännu inte finns någon rättspraxis. För multinationella företag har det tidvis varit knepigt eftersom de nationella dataskyddsmyndigheterna kan lägga upp egna riktlinjer och tolkningar. Man måste införa nationella specialvillkor vilket kräver en massa arbete. Person Y anser ändå att detta kommer gynna multinationella företag i framtiden.

Har sättet som ni kommunicerar med era kunder på förändrats?

Som tidigare nämnt säger person X att det har skett stora förändringar genom den nya kundplattformen. De försöker lära ut till sina kunder vad som är rekommenderas och vad som bör undvikas. Det gör de för att minimera antalet personuppgifter som rör sig via mindre säkra kanaler. De har även en stor aktsamhet med hur de själva utbyter information med andra.

Person Y säger att det har skett ändringar exempelvis inom marknadsföringskommunikationen. Främst i form av att det behövs ett dokumenterat samtycke mellan parterna. På grund av detta anser Person Y att det kommer gynna företaget eftersom det sker en koncentrering av deras marknadsföring till konsumenterna. Kundservicen och kommunikationen är fortfarande på samma nivå som före förordningen togs i bruk. Det som har ändrat är att e-posten inte alls används för att dela information som innehåller personuppgifter. De har istället en säkrare plattform för informationsbyte med kunderna, som redan var i användning före GDPR, men som nu används ännu mer.

Har sättet som ni lagrar information på ändrat?

Person X berättar att de som ett resultat av minimeringen av e-posten också undviker att spara information där. Informationen sparas istället på en annan plattform. Person X säger även som tidigare nämnt att på grund av splittringen mellan bokförarna och lönesidan så strävar företaget efter att de anställda endast skall ha tillgång till den lagrade informationen de själva behöver. Merparten av deras lagrade data är sparat på en server och i samband med GDPR har de även startat en ny server för endast löneräknarna. Person X betonar att det handlar till stor del om rättigheter, dvs de som inte har behov av lönematerialet skall heller inte ha tillgång till det.

Person Y berättar att all den information som innehåller personuppgifter inte längre skickas med e-post och lagras på så vis inte där heller. All information lagras istället på företagets egen plattform som är betydligt säkrare. För marknadsföringskommunikationen dokumenteras samtycke då det kommer till kunder samt potentiella nya kunder.

Har personalen utbildats?

Person X säger att företaget har satsat en hel del på utbildning för personalen. De har ordnats både skolningar och seminarier. Det har fokuserats på att personalen skall ha en klar bild av vart företaget är på väg samt utbilda dem i hur GDPR konkret påverkat deras arbete och arbetsrutiner. Person X nämner att man tror att folk har varit mycket rädda för förordningen men att det sist och slutligen inte har skett så stora ändringar. Person X säger att de största ändringarna ändå har skett på ett högra plan där de har varit tvungna att förnya deras avtalsvillkor och lägga till bilagor. De har alltså förnyat avtalen med sina kunder. Det är ett skilt GDPR-team som har ansvarat för att göra ett register och skriva om hur personuppgifterna behandlas inom företaget. Person Y berättar att en allmän GDPR-utbildning ar erbjudits till personalen. Dessutom har man träningssessioner för arbetsspecifika ändamål.

Hur har era kunder reagerat?

Person X säger att det har rått en viss oro över hur saker och ting skall fungera med den nya reformen. En del kunder har även ansett det krångligt att de inte längre kan använda e-posten till allt deras informationsbyte. Medan de flesta kunderna förstår att det är någonting som måste göras och att det inte är företaget själv som har beslutat om GDPR, har de ändå fått en del negativ feedback från sina kunder. Person X nämner även att det också sker andra förändringar, exempelvis ”katso”-rättigheterna som skall tas i bruk i början av 2019. Det

leder lätt till att kunderna anses det vara jobbigt att företaget hela tiden kräver nya rättigheter av kunderna tillika som nya system måste inrättas. Person X antar ändå att kunderna i grund och botten förstår att det är saker som måste göras och att det inte är företagets egna idéer. Person X betonar hur viktigt det är att kommunicera med kunden och på ett bra sätt förklara vad som sker och varför. Då har kunderna lättare att förstå varför saker görs och av vilken anledning.

Person Y berättar att kunderna i huvuddrag har reagerat positivt till förändringarna. Det är främst deras mindre kunder som ibland har haft svårt att förstå vad GDPR innebär och hur det påverkar deras arbete. Person Y anser ändå att det har varit fördelaktigt att i samband med GDPR har företagets kunder varit mer engagerade i säkerhets- och dataskyddsproblem. Det är trots allt på kundernas eget ansvar att de sköter sin del.

Har ni haft problem med kunder som inte följer era instruktioner?

Peson X säger att det finns en tydlig skillnad mellan företagets kunder. Ett stort företag har ofta lättare att förstå att allt måste vara i skick. De mindre kunderna är de som främst haft problem med att inte använda e-post. Person X nämner dock att det inte någonstans finns specificerat att man inte skulle få använda e-post, utan det handlar om att företaget självt ansett att det inte är en säker kanal för informationsbyte. Jag frågade av person X varför man anser att e-post inte är en säker kanal och fick till svar att den är för lätt att komma åt. Även om chanserna är små finns det risk för att en hackare går in i e-posten och exempelvis laddar ner PDF-filer, vilket inte lämnar några tydliga spår efter sig. Person X nämner säkrad e-post som ett alternativ till den vanliga e-posten.

Person Y berättar att det inte har förekommit sådana fall. Företaget ger tydliga riktlinjer till kunderna för att hjälpa dem att uppfylla sina krav. Om det skulle gå så att kunden inte följer det som bestämts i förordningen, är det på kundens eget ansvar. Företagets kunder är även själva skyldiga för eventuella juridiska konsekvenser, exempelvis böter. Om någon av företagets kunder skulle råka ut för en sådan process anser person Y att det nog skulle kunna bli en stor belastning också för dem.

Har GDPR medfört mycket kostnader?

Person X berättar att GDPR absolut har medfört kostnader. Det har gått åt en hel del arbete till att exempelvis förnya avtalen och skriva om bilagorna. Kostnader har även uppkommit i

samband med inskolningen av personalen. De är de själva på kontoret som faktiskt är ansvariga för att kunderna skriver på de nya avtalen. Det har också uppstått kostnader i samband med implementeringen av de nya plattformarna. Det är både företaget och kunden som blir belastade av de kostnaderna. Person X tror inte att förordningen i framtiden kommer att spara in något, eftersom det främst har påverkat hur man kommunicerar med kunderna.

Person Y berättar som tidigare nämnt att det i förberedningsfasen har uppstått en hel del extra kostnader. De har även köpt en ny tjänst för att försäkra att den information som skickas behålls på servrar inom EU. Kostnaderna kan sedan i sin tur sparas in då man hjälper kunderna med att följa de registeransvariga skyldigheterna som uppstått. Person Y anser också att man på grund av de rediga system samt dokumentationen som nu byggs upp, räknar med att kunna spara in ganska mycket i framtiden.

7 Analys och resultat

Hur har bokföringsbyråerna i Finland påverkats av GDPR? Vad har bokföringsbyråerna gjort för att anpassa sig?

GDPR förordningen, som introducerades redan 2012 och röstades igenom 2016, trädde i kraft 25 maj 2018. Det betyder att alla företag har haft en lång tid att förbereda sig på att se till att alla arbetsrutiner är i enighet enligt den. Person Y tar i alla fall upp att deras företag har jobbat med förordningen redan i flera år och att man redan uppfyllde en del av kraven som infördes. Han nämnde också att arbetet inte på något vis är klart, utan att det krävs ständiga uppdateringar för att se till att allting sköts på rätt sätt. Kapitel 4.5 tar upp teori om e-post och hur den inte är det säkraste sätter för informationsbyte mellan tjänsteleverantör och kund. I företag X minimerar man användning av e-post. Man undviker även att ta emot information som innehåller personuppgifter av sina kunder. I företag Y använder man inte överhuvudtaget e-post för att själv skicka eller ta emot information av kunder. Båda företagen använder istället en egen säkrare plattform. Här hittas en klar sammankoppling mellan teori och intervjupersonernas svar.

Kapitel 3 tar upp hur viktigt det är att endast de som behöver någon specifik lagrad information har tillgång till den. All den information en bokföringsbyrå har lagrad och som innehåller personuppgifter ska alltså inte vara tillgänglig för hela personalen om inte alla behöver den. Person X berättade under intervjun att man i företaget har spjälkat upp bokförings- och lönehanteringsavdelningen så att bokförarna inte har tillgång till de känsliga personuppgifterna på lönehanteringsavdelningen. Om en bokförare sedan exempelvis

bokslutet behöver någon av den oåtkomliga informationen måste man be separat om den av löneräknarna. Då skalas personuppgifterna bort så att endast siffrorna är tillgängliga. Laglig behandling av personuppgifter behandlas i kapitel 3.2. Både person X och person Y berättar om hur man har gjort nya avtal med sina kunder, som innehåller nya bilagor, för att få behandlingen dokumenterad. Dokumentering och ständig uppföljning är en av kärnpunkterna i GDPR.

I kapitel 4 skrivs det om intern kontroll, risker och riskbedömning. För att ett företag skall kunna kontrollera säkerhetsnivån krävs det ständig uppföljning av vilka risker som finns i spel och hur man skall hantera dem. Person Y berättat att de fortfarande jobbar med riskbedömning. Arbetsrutinerna måste ständigt uppföljas så att man hela tiden är medveten om hur det aktuella läget är angående säkerheten. Företag Y jobbar med att kartlägga de långvariga riskerna och hur man skall hantera dem.

Kapitel 4.3 handlar om säkerhet vid behandling. Där skrivs det om hur viktigt det är med en hög säkerhetsnivå. Både företag X och företag Y lägger stor vikt vid säkerheten. Det att både kunden och tjänsteleverantören anser att säkerheten hålls på en hög nivå är fördelaktigt för båda parterna. Person Y nämner dessutom hur införandet av GDPR har lett till en förbättring av säkerheten som helhet, inte endast inom dataskyddet. I kapitel 4.5.2 är det också skrivet om att den delen av personalen i ett företag som behandlar personuppgifter eller känsliga personuppgifter måste utbildas i sina arbetsrutiner. Det kommer klart fram av båda intervjupersonerna att man inom företagen har satsat en hel del på att utbilda personalen.

Bokföringsbyråer behandlar en stor mängd personuppgifter. Det kommer klart fram i intervjuerna att det har skett ett omfattande arbete i samband med implementeringen av GDPR. Efter den 25 maj 2018 sköts arbetet på ett annorlunda sätt på bokföringsbyråerna. Det man kan konstatera är att medborgarna nu är säkrare än förut, åtminstone om man ser på hur två av de stora bokföringsbyråerna i Finland nuförtiden gör sitt arbete. ’

8 Slutsatser

I analysen och resultatet fördes det fram de sammankopplingar som finns mellan teorin och den kvalitativa undersökningen. Som beskrivet finns det tydliga sammankopplingar och man kan se att åtminstone de stora bokföringsbyråerna som är med i min undersökning har följt GDPR noggrant. Med tanke på hur förödande straffet kan bli för den som inte följer förordningen, är det förståeligt att företagen tar det på största allvar. Syftet med intervjuerna var att ta reda på hur och vad företagen konkret har gjort för att följa förordningen. Det

officiella GDPR-dokumentet lämnar en del att tolka vilket gör det intressant att se vilka åtgärder företagen har tagit till för att följa det. Till de största ändringarna hör de ändringar företagen gjort när det kommer till kommunikation och informationsbyte med kunden. En central del är också det att man sett över sina arbetsrutiner, så att personer endast har tillgång till den information som de faktiskt behöver. Även det att man i båda företagen har kunnat konstatera att det inte bara är hanteringen av personuppgifter, utan snarare hela den interna säkerheten har uppnått en högre nivå i samband med det nya regelverket. Sist och slutligen har förändringen i arbetsrutinerna inte varit särskilt stora, men de har blivit mycket säkrare för både tjänsteleverantör och kund.

9 Kritisk granskning

I detta kapitel utför jag en kritisk granskning av mitt examensarbete. I den empiriska delen använde jag mig av endast två intervjuer. Flera intervjuer kunde mycket väl ha gett en ännu bredare bild av förändringarna inom bokföringsbyråerna. Jag valde att inte göra fler intervjuer eftersom jag själv ändå ansåg att jag fick all den information jag behövde från mina intervjuer. En annan sak som bör tas i beaktande är att GDPR-förordningen lämnar mycket att tolka. Eftersom arbetets skrivits en relativt kort tid efter ibruktagandet av det nya regelverket är de fullt möjligt att arbetet skulle se annorlunda ut om det gjordes exempelvis fem, eller tio år, efter ibruktagandet.

Man skulle även kunna få en större helhetsbild av förändringarna inom bokföringsbyråerna om man tog i beaktande även mindre företag. I min undersökning har jag avgränsat mig till att undersöka endast de största aktörerna på marknaden, men det är fullt möjligt att situationen skulle se annorlunda ut i mindre företag.

10 Avslutande diskussion

I arbetet har jag undersökt vad GDPR är och vilka ändringar som träder i kraft till följd av förordningen. Teorin har kretsat behandlat personuppgifter och känsliga personuppgifter definieras, hur de lagligt behandlas enligt GDPR samt hur de påverkar bokföringsbyråerna. Det intressanta är att GDPR kommer med riktlinjer, men lämnar ändå en hel del att tolka.

Jag har intervjuat två personer med olika positioner i olika företag. Frågorna och kompletterade den teoretiska delen. Det finns klara sammankopplingar mellan teorin och intervjupersonernas svar. Svaren tyder på att företagen länge har förberett sig för förordningen, men att de fortfarande måste jobba för att se till att företaget uppfyller kraven.

Eftersom dokumentering är en central del av förordningen krävs det ständig uppföljning. Resultatet tyder på att i alla fall de stora företagen inom branschen har påverkats och lagt ner mycket tid på att följa det som bestämts i samband med förordningen. Vidare forskning kunde göras till exempel genom att undersöka hur de mindre företagen med mindre resurser har gjort i fråga om till GDPR-förordningen. Dessutom kunde man forska i hur det har påverkat företagen, alltså tjänsteleverantörernas kunder, och vad de har gjort för att anpassa sig till GPDR samt hur det har påverkat deras arbete.

Källförteckning

Bryman, A. &. B. E., 2013. *Företagsekonomiska forskningsmetoder.* Stockholm: Liber Ab.

Datainspektionen, u.d.. *Datainspektionen - Anmäl personuppgiftsincidenter.* [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/anmala-personuppgiftsincident/
[Accessed 12 2018].

Datainspektionen, u.d.. *Datainspektionen - De registrerades rättigheter.* [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/de-registrerades-rattigheter/
[Accessed 12 2018].

Datainspektionen, u.d.. *Datainspektionen - Informationssäkerhet.* [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/
[Accessed 12 2018].

Datainspektionen, u.d.. *Datainspektionen- Säkerhet för personuppgifter i e-post.* [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/sakerhet-for-personuppgifter-i-e-post/
[Accessed 12 2018].

Datainspektionen, u.d.. *Datainspektonen - Säkerhet för personuppgifter i e-post.* [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/sakerhet-for-personuppgifter-i-e-post/
[Accessed 12 2018].

eugdpr, u.d.. *eugdpr - The European Union Legislative Process.* [Online]
Available at: https://eugdpr.org/the-process/
[Accessed 12 2018].

europa, 2018. *europa - Förordningar, direktiv och andra rättsakter.* [Online]
Available at: https://europa.eu/european-union/eu-law/legal-acts_sv
[Accessed 10 2018].

europa, u.d.. *europa - Vad är en personuppgiftsansvarig eller ett personuppgiftsbiträde?.* [Online]
Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_sv
[Accessed 10 2018].

foretagarna.se, 2018. *foretagarna.se.* [Online]
Available at: https://www.foretagarna.se/juridisk-faq/ovrigt/gdpr-live-fragor/
[Använd 03 2019].

GDPR, 2016. *GDPR.* [Online]
Available at: https://www.gdpr.associates/wp-content/uploads/2017/05/Swedish-CONSIL3AST_5419_2016_INIT3ASV3ATXT.pdf
[Accessed 11 2018].

GDPR, 2018. *GDPR.* [Online]
Available at: https://www.gdpr.associates/wp-content/uploads/2017/05/Swedish-CONSIL3AST_5419_2016_INIT3ASV3ATXT.pdf
[Accessed 10 2018].

Investopedia, 2019. *Investopedia - General Data Protection Regulation (GDPR).* [Online]
Available at: https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp
[Accessed 10 2019].

Samlogic, u.d.. *Samlogic - Hur påverkar nya dataskyddsförordningen (GDPR) företag och organisationer?.* [Online]
Available at: http://www.samlogic.com/articles/gdpr-eu-dataskyddsforordningen-foretag-organisationer.htm
[Accessed 10 2081].

Sentor, u.d.. *Sentor - EN SNABBARE VÄG MOT.* [Online]
Available at: https://www.sentor.se/informationssakerhet/dataskyddslagen-gdpr-forstudie/
[Accessed 11 2018].

Slideplayer, 2018. *Slideplayer.* [Online]
Available at: https://slideplayer.se/slide/14878196/
[Accessed 01 2019].

ssrma, u.d.. *ssrma - Risk management in self storage operations.* [Online]
Available at: http://ssrma.org/risk-management/
[Accessed 01 2019].

Westerlund, M., 2018. *A Study of EU Data Protection Regulation and Appropriate Security for Digital Services and Platforms.* Åbo: Åbo Akademi Universety.

Wikland, B., 2014. *Intern styrning och kontroll - Både lönsamt och säkert.* Stockholm: FAR Akademiu AB.

www.cygate.se, 2017. *Cygate - GDPR.* [Online]
Available at: https://www.cygate.se/blogg/gdpr-sa-forbereder-sig-cygate/
[Accessed 10 2018].

Figurförteckning

Bilaga 1 Intervjufrågor

1. Har det skett konkreta ändringar i ert arbete pga. GDPR?

- Arbetsrutiner? Kommunikation med kunden?

2. Har GDPR medfört fördelar till ert arbete?

- Säkerhet? Intern kontroll?

3. Har GDPR medfört nackdelar?

- Kostnader? Försvåring av arbete?

4. Har sättet som ni kommunicerar med era kunder på förändrats?

- E-post? Övriga plattformar?

5. Har sättet som ni lagrar information på ändrat?

- E-post? Molntjänster?

6. Har personalen utbildats?

- Seminarier? På egen tid? När/distansskolningar?

7. Hur har era kunder reagerat?

- Positiv/negativ feedback?

8. Har ni haft problem med kunder som inte följer era instruktioner?

- Problem med att skriva nya avtal?

9. Har GDPR medfört mycket kostnader?

- Kortsiktiga kostnader? Räknar man med att spara in i framtiden?