Examensarbete

HÖGSKOLAN I SKÖVDE

GDPR OCH BACKUPER HOS MJUKVARUUTVECKLINGSFÖRETAG

En kvalitativ intervjustudie

GDPR AND BACKUPS AMONG SOFTWARE DEVELOPMENT COMPANIES

A qualitative interview study

Examensarbete inom huvudområdet informationsteknologi med inriktning mot Nätverks- och systemadministration

Grundnivå 22,5 Högskolepoäng
Vårtermin 2018
IT610G

Ted Johansson

Handledare: Johan Zaxmy
Examinator: Rose-Mharie Åhlfeldt

Summary

The purpose of this work is to check how companies have been adapted to the General Data Protection Regulation, both in terms of routine work and changes that they have implemented. The work addresses how companies have changed their routines regarding backups of critical business data and routines about the right to be forgotten.

At the end of this work, the GDPR will come into force (25th of May 2018) and therefore all activities should have implemented some form of change in view of the changed legislation that will apply. Since GDPR is a new legislation (which has been up to date in the past 2 years), some work is being done about just GDPR and what business changes should be made. However, no focus has been on how companies should adapt their routines about backups and how businesses should reason about the right to be forgotten. This makes this work very relevant as this is something that many businesses should have changed, thought about and documented.

The method used in this study is a qualitative form, in which interviews have been conducted with representatives from different activities in the development industry. The businesses sell their software and services to customers, and they often handle large amounts of personal information that either passes through the systems or is stored with them. The organizations interviewed have been working for GDPR for a while. In several of the cases a year back to ensure that their actions are in line with the GDPR.

Five interviews were conducted in full. Then a thematic analysis has been conducted on the results of the interviews. The interviews focus on whether and what changes the companies have made and how it looks today. Following the analysis, it is clear that companies have made certain changes in the organization, but to a large extent these changes have only been conducted in terms of checking where information is available and documentation about this and the different routines available at the company.

Keywords: GDPR, General Data Protection Regulation, Backups, Backup, Routines

Sammanfattning

Detta arbete har som syfte att kontrollera hur verksamheter har anpassat sig inför General Data Protection Regulation (GDPR, sv. Dataskyddsförordningen), både vad det gäller rutinarbete och förändringar som de har genomfört. Arbetet behandlar hur företagen har förändrat sina rutiner gällande säkerhetskopior av kritisk företagsdata och även rutiner kring rätten att bli bortglömd.

Vid detta arbetes slut kommer GDPR har trätt i kraft (25:e maj 2018) och därmed bör samtliga verksamheter ha genomfört någon form av förändring inför den ändrade lagstiftningen som börjar gälla då. Då GDPR är en ny lagstiftning (som dock varit aktuell de senaste 2 åren) finns en del arbeten kring just GDPR och vilka verksamhetsförändringar man bör vidta. Dock har inget fokus skett på hur företag bör anpassa sina rutiner kring säkerhetskopior och hur företagen bör resonera kring rätten att bli glömd. Därmed blir detta arbete väldigt aktuellt då detta är något som många verksamheter bör ha förändrat, tänkt på och dokumenterat.

Metoden som använts i denna studie är en kvalitativ form, där intervjuer har genomförts med representanter från olika verksamheter inom utvecklingsbranschen. Verksamheterna säljer sina programvaror och tjänster till kunder och de hanterar därmed ofta stora mängder personlig information som antingen passerar igenom systemen eller som lagras hos de. Organisationerna som intervjuas har jobbat med GDPR ett tag. I flera av fallen ett år tillbaka för att säkerställa att de deras åtgärder överensstämmer med GDPR.

Fem intervjuer genomfördes i sin helhet. Därefter har en tematisk analys genomförts på resultatet från intervjuerna. I intervjuerna är fokus på om och vad för förändringar företagen har genomfört samt hur det ser ut i dagsläget. Efter analysen framträder tydligt att företagen har genomfört vissa förändringar i organisationen, men till större del har dessa förändringar enbart genomförts i form av kontroll av var information finns och dokumentation kring detta och de olika rutiner som finns vid företaget.

Nyckelord: GDPR, General Data Protection Regulation, Säkerhetskopior, Backup, rutiner

Begrepp och förkortningar

GDPR – General Data Protection Regulation (Sv. Dataskyddsförordningen)

IT – Informationsteknologi

PUL – Personuppgiftslagen

EU – Europeiska Unionen

Innehåll

1. Introduktion 1

2. Bakgrund 2

2.1 Behandling 2

2.3 PUL 2

2.4 GDPR 2

2.4.1 Dataskyddsombud 4

2.4.2 Dataportabilitet 4

2.4.3 Rätten att bli bortglömd (RABB) 4

2.4.4 Samtycke och laglig grund 4

2.4.5 Avtal och ansvarig/biträde 5

2.4.6 Klagomål/skadestånd 5

2.4.7 Persondata och känsliga persondata 5

2.4.8 Backuper och GDPR 6

2.4.9 Rutiner 6

2.5 Backup 6

2.5.1 Backupmetoder 7

2.5.2 Vilken data säkerhetskopieras? 8

2.5.3 Redigering av backuper? 9

3 Problembeskrivning 10

3.1 Utmaningar med GDPR och backuper 10

3.2 Rutiner 10

3.3 Frågeställning 11

3.4 Syfte 11

3.4 Avgränsning 12

3.5 Förväntat resultat 12

4 Metod 13

4.1 Val av metod 13
4.2 Intervjustudie 13
4.3 Övergripande literaturgranskning 14
4.4 Frågekonstruktion 14
4.5 Validitet 15
4.6 Etik 15
4.7 Urval 16
4.8 Metodsteg 16
4.9 Genomförande 17
4.10 Transkribering 17
4.11 Analys 18
5. Resultat 19
5.1 Presentation av verksamheterna och respondenterna 19
Respondent 1 19
Respondent 2 19
Respondent 3 19
Respondent 4 19
Respondent 5 19
5.2 Sammanfattning 20
5.2.1 På vilket sätt har verksamheterna förändrat sin rutin för säkerhetskopieringen? 20
5.2.2 Hur har verksamheterna utformat sin rutin för ifall någon vill bli bortglömd med avseende på era backuper? 21
5.2.3 Hur har verksamheterna rent tekniskt förändrat säkerhetskopiering av datan? 22
5.2.4 Hur ser verksamheterna på framtiden vad gäller säkerhetskopiering och rätten att bli glömd? 23
6. Analys 24
6.1 Tema 1 – Rutiner vid säkerhetskopiering 24
6.2 Tema 2 – Rätten att bli glömd 26

6.3 Tema 3 – Tekniska förändringar av säkerhetskopieringar 27

6.4 Tema 4 – Framtiden och andra företag 28

7. Slutsats 30

8. Diskussion 31

8.1 Samhällsnytta 33

8.2 Etiska Aspekter 33

8.3 Framtida arbete 33

Referenser 35

Bilaga A – Intervjuunderlag

Bilaga B – Rutiner vid säkerhetskopiering

Bilaga C – Rätten att bli glömd

Bilaga D – Tekniska förändringar av säkerhetskopieringar

Bilaga E – Framtiden och andra företag

1. Introduktion

Den 25 Maj 2018 införs GDPR (sv. Dataskyddsförordningen) i Europa, därmed tillkommer nya krav och lagar för verksamheter att rätta sig efter. Utöver detta får de även ökat ansvar för uppgifterna och även större kontroll till privatpersoner. Lagen kan omfatta stora processer inom verksamheter som behöver anpassa sig och göra sig redo för att möta de lagkrav som kommer.

Då många verksamheter idag hanterar personuppgifter kommer det krävas att de rättar sig efter GPDR för att undvika påföljder. Detta sker som ett led i en rad förändringar som kommer genomföras, allt för att stärka den personliga integriteten hos den Europeiska befolkningen. Idag har den personliga integriteten urholkats kraftigt. Ett exempel på detta är Facebook och Cambridge Analytica skandalen där 87 Miljoner invånare i USA har blivit kartlagda genom deras information som de delar på Facebook med hjälp av en applikation kopplad till tjänsten (Lindhe, 2018). GDPR ämnar därför att återge kontrollen över personuppgifterna till den som faktiskt är ägaren av de.

Något man sällan tänker på är informationen bakom allting. Säkerhetskopiorna på all information som finns på internet som företag lagrar för att kunna återställa i händelse av systemkrascher, korrupt information och förlorade filer. Utöver denna information finns även stora databaser där transaktioner flödar och lagras i databasen. Dessa kritiska system tas ofta kontinuerliga säkerhetskopior på för att skydda data, men vilken information ligger verkligen där? Detta arbete behöver nu företag ta reda på och dokumentera inför GDPR.

Inför GDPR behövs dokumentation och ändringar genomföras innan datumet lagen börjar gälla, men vad behöver man göra och hur skall man göra det? Det är något som flera företag ställer sig frågande till. Informationen som företagen innehar är utav blandad form, men den som klassas som personuppgift måste skyddas (Tankard, 2016). Därför ämnar denna rapport kontrollera vad företagen har genomfört för förändringar inför GDPR. Fokuset kommer därför vara vilka förändringar de har genomfört gällande sina backuprutiner och även rutiner kopplade till det som har med rätten att bli glömd att göra.

Genom att undersöka hur olika verksamheter inom utvecklingsbranschen har anpassat sig inför det stundande införandet av GDPR kan man därmed se hur och vad de har gjort för att säkra den latenta information de innehar. För att få reda på informationen kommer en intervjustudie genomföras. Organisationerna som intervjuas har en blandad ålder i branschen men kunskapen bör finnas där för att de skall kunna möta lagkraven som ställs på det från den 25:e maj.

2. Bakgrund

Följande stycke kommer inledningsvis behandla PUL som är den nuvarande lagstiftningen som behandlar hanteringen av personuppgifter, därefter behandlas GDPR och de stycken som relaterar till det ämne denna rapport ämnar svara på. Därefter kommer konceptet kring backuper att förklaras och gås igenom för att skapa en bild av hur dessa relaterar till varandra.

2.1 Behandling

En central del i dagens samhälle är information om personer och organisationer. Vissa företag livnär sig till fullo på detta och denna data delas t.ex. från olika undersökningar som genomförs på internet. Behandling är när man genomför en åtgärd eller flera åtgärder mot insamlade personuppgifter eller en samling personuppgifter på något sätt (Datainspektionen, 2018e). Exempel på detta är att skicka ut nyhetsbrev, reklam eller analysera en profil (profilera) för att se om en person är lämpad som kund eller partner. Den information som behandlas kan vara allt ifrån personers ålder och kön till företags in-och utgifter behandlas för att skapa underlag, det senare kan vara för att skapa sk. ”leads” inom olika affärsintelligens-system för potentiella kunder. Vid denna behandling av personuppgifter krävs det att man rättar sig efter vissa lagar.

2.2 PUL

Personuppgiftslagen (1998:204) är gällande lag fram till dess att GDPR träder i kraft. Dess syfte är att skydda svenska medborgares personliga integritet genom att stipulera hur personuppgifter skall hanteras. PUL grundar sig på dataskyddsdirektivet, där det är ett direktiv är medlemsländerna inte tvingande att anta lagen i fullo enligt detta, utan snarare att de skall nå ett visst mål som överensstämmer med direktivet (Wester-Lindgren, 2017). PUL ersätts till fullo av GDPR den 25:e maj, då den europeiska lagstiftning ersätter den svenska.

Värt att nämna om PUL är att den har inte haft den pondus och laga kraft för att se till att lagen följs (Sveriges Radio, 2018). Utöver detta, när överträdelser väl har skett har det sällan blivit några repressalier tack vare PUL (EU:s nya dataskyddsförordning GDPR - Fortnox, 2018).

2.3 GDPR

GDPR är en europeisk förordning som ämnar att harmonisera behandling av personuppgifter som rör europeiska medborgare. Denna behandling gäller både inom och utom europiska gränser och det finns även stipulerat vad som gäller vid utlämning eller behandling av data till tredje land. Med förordning menas att detta blir en direkt nationell lagstiftning som medlemsländerna skall följa, den är alltså ”direkt tillämplig” (Wester-Lindgren, 2017).

”The Final European Union General Data Protection Regulation” (BURTON, et al. 2016) behandlar vad de nya Europeiska reglerna faktiskt betyder för verksamheter, hur dessa kan tolkas och hur man skall ställa sig till dessa. De behandlar även vilka vägar som lagen tagit, t.ex. om den har förändrat sig sedan den första iterationen till den slutgiltiga versionen av GDPR, denna har förändrats ett antal gånger sedan den först lades fram.

Det som gör GDPR unik och verkningsfull är till stor del genom de stora sanktionsavgifter som organisationer kan drabbas av vid potentiella överträdelser av lagstiftningen. Dessa kan uppgå till som högst 4% av den totala omsättningen eller 20 miljoner € beroende på allvarligheten i

överträdelsen som skett (Datainspektionen, 2018d). Självklart påverkas bötessumman beroende på vilken typ av överträdelse som skett och hur grav denna här.

Utöver detta kräver GDPR att vid större hantering utav personuppgifter krävs dokumentation och utsedda ansvariga vid organisationen. I dokumentationen skall det tydligt framgå uppgifter om vem som är dataskyddsombudet vid organisationen, i vilket ändamål behandlingen av personuppgifter sker, hur den sker, vilka uppgifter som behandlas och slutligen (Datainspektionen, 2017g) (om möjligt) hur uppgifterna skyddas. Detta krav ställs när en organisation omfattar mer än 250 personer eller om behandlingen av uppgifterna kan medföra risk för de vars data behandlas.

Det som skiljer sig som mest åt från PUL som finns i Sverige idag är framförallt de straff som finns och hur behandling får ske. Utöver detta har kraven på hur länge personuppgifter får lagras ändrats så att laglig grund alltid måste finnas för behandling av personuppgifter. Ifall dessa ej finns behov av längre skall dessa raderas inom ett år ifall laglig grund ej finns för fortsatt behandling av uppgifterna.

Utöver detta finns även en ökad anmälningsplikt vid potentiella intrång, specifikt där det finns risk att personers data har blivit åtkomlig för någon annan part än den som är avtalad. Detta skall då anmälas till den lokala tillsynsmyndigheten inom 72 timmar, samt de personerna som kan ha blivit drabbade av intrånget (Datainspektionen, 2018a). I Sverige är denna myndighet datainspektionen (Datainspektionen, 2017 B) och de ansvarar för att GDPR efterlevs och dataskyddslagen som behandlar de anpassningar Sverige gör utifrån den anpassningsmöjlighet som finns i GDPR.

När det kommer till långtidsförvaring av data som ej behandlas, utan ligger i ett arkiv, finns det inget i lagtexten som direkt stipulerar vad som får göras med denna, eller vad som skall göras mer än den lagliga grunden och den tid som samtycke finns. Ifall data behövs för till exempel bokföring eller liknande må data sparas i upp till sju år (Bokföringsnämnden, 2017) men därefter skall denna raderas. Det finns alltså lagar och förordningar som går över GDPR. Exempel på detta är t.ex. bokföringslagen som anger att ekonomiska transaktioner måste sparas i minst sju år, trots att det kan finnas namn och liknande på dessa.

Kärnan i GDPR är just samtycke och rätten att bli bortglömd. Dessa tillhör en mängd nya rättigheter som europeiska medborgare får (Datainspektionen, 2017 C):

Rätt till information: Den registrerade har rätt till information om när dennes uppgifter behandlas.
Rätt till rättelse: Den registrerade har rätt att vända sig till företag och få sina uppgifter rättade.
Rätt till radering: Den registrerade har rätt att vända sig till företag eller myndighet och be att uppgifterna som rör den egna personen att bli raderade eller borttagna inom rimlig tid.
Rätt till begränsning av behandling: i vissa fall kan enskild begära att ens data enbart får hanteras vid specifika tillfällen, t.ex. vid begäran om rättelse skett.
Dataportabilitet: data skall försvaras på ett sådant sätt att det lätt går att begäras ut och flyttas till en annan personuppgiftsansvarig.
Rätt att göra invändningar: Den registrerade har rätt att invända mot hanteringen av dennes uppgifter, då skall den personuppgiftsansvarige avstå från behandling såvida detta ej går att bevisa att intresset att behandla dennes uppgifter överstiger dennes intressen och rättigheter.
Automatisera beslutsfattning (profilering):
Klagomål: Den som anser att ens uppgifter blivit felaktigt behandlade kan lämna klagomål till datainspektionen, de avgör i fallet om en tillsyn skall göras.

Skadestånd: Om den registrerades uppgifter behandlats felaktigt kan denne begära skadestånd av den eller de personuppgiftsansvariga som medverkat vid behandlingen.

2.3.1 Dataskyddsombud

I de fall en organisation hanterar en stor mängd personuppgifter kan ett dataskyddombud behöva utses. Ombudet har till uppgift att kontrollera att organisationen följer GDPR genom informationsspridning och kontroller inom organisationen. En fördel är om personen i fråga är opartisk till stor del samt att den har tillräckligt att säga till om inom organisationen för att kunna genomföra förändringar ifall potentiella felaktigheter sker gentemot GDPR.

Datainspektionen (2017g) nämner ett antal kriterier för vem som kan vara dataskyddsombud, genomgående är att personen måste få de resurser den behöver för att kunna genomföra uppdraget och upprätthålla GDPR inom organisationen. Personen som blir utsedd till dataskyddsombud har ett antal uppgifter utöver de som nämndes inledningsvis, t.ex. att vara kontaktperson för datainspektionen och kontaktperson för de registrerade. Dessutom skall personen som nämndes tidigare kontrollera verksamheten och se till att den följer de bestämmelser och riktlinjer som fastställts.

2.3.2 Dataportabilitet

Med dataportabilitet menas att man vid behov och vid särskilda omständigheter har rätt till att flytta sina uppgifter från en hanterare till en annan, t.ex. från ett socialt nätverk till ett annat (Datainspektionen, 2017 C). Detta tillammans med rätt att bli bortglömd gör att ägaren till personuppgifterna som behandlas kommer ha mycket större kontroll över hur och var ens uppgifter finns och vad som görs med dessa.

2.3.3 Rätten att bli bortglömd (RABB)

Med denna lagstiftning åtnjuter den enskilde medborgaren och medlemmen i ett europeiskt land större kontroll än tidigare, detta då denna lag innebär att man inom skälig tid skall kunna bli borttagen ur ett företags samtliga system, genom att återkalla rätten företaget har att behandla ens personuppgifter (Datainspektionen, 2017e). Utöver detta har den enskilde även rätt att begära ut vem som ens uppgifter lämnats ut till för vidare behandling vid nyttjande av sin rätt. Utöver detta skall den som varit personuppgiftsansvarig meddela de företag som man delat personens uppgifter med att den registrerade vill bortglömd, det sistnämnda gäller dock enbart om detta ej är för betungande.

Borttagningen gäller ej om det behövs för att uppfylla yttrande- och informationsfriheten eller andra rättsliga delar, som myndighetsutövning.

2.3.4 Samtycke och laglig grund

För att få behandla personuppgifter behövs en laglig grund till behandlingen av uppgifterna. Detta kan inhämtas på flera sätt men genomgående är att detta måste inhämtas explicit, alltså ej en för i-bockad ruta i ett formulär utan samtycket behöver ske genom en aktiv handling.

Några av de delar som måste uppfyllas för att godkännas som laglig grund är följande (SOU 2017:39, 2017):

- Samtycke
- Det krävs för att kunna fullgöra avtal
- Nödvändig för rättslig förpliktelse
- För att skydda intressen utav grundläggande betydelse för den registrerade
- Utföra en uppgift av allmänt intresse

En central del i GDPR är att den registrerade har gett sitt uttryckliga samtycke till att behandling av dennes uppgifter får ske (SOU 2017:39, 2017). Behandlingen av personens uppgifter faller då in under ”laglig behandling”. Detta samtycke kan när som helst återkallas och därmed får uppgifterna som lämnats ut ej behandlas mer.

2.3.5 Avtal och ansvarig/biträde

Vid behandling av personuppgifter i verksamheter faller det sig ofta att företag är de som blir personuppgiftsansvariga för sina anställda, detta då de arbetar där och deras uppgifter behövs behandlas för att kunna betala ut lön osv. När ett företag ingår ett avtal med ett annat företag behövs det finnas avtal mellan parterna som kallas ett ”personuppgiftsbiträdesavtal”. Företaget godkänner då att det andra företaget behandlar vissa uppgifter när det behövs för att kunna uppfylla avtalet. I det avtal som skrivs anges vad som får göras med uppgifterna och vilka uppgifter man har rätt att tillgå. Ett exempel på detta är om en molntjänst skall införskaffas från ett annat företag, dessa blir då biträden till företaget som är personuppgiftsansvarig (Datainspektionen, 2018f).

Ett biträde är en fysisk eller juridisk person eller t.ex. offentlig myndighet som får behandla de uppgifter som anges i personuppgiftsbiträdesavtal vid de tillfällen som anges i avtalet.

2.3.6 Klagomål/skadestånd

Ifall en enskild person anser att felaktig behandling skett, som går i strid med vad som anges i dataskyddsförordningen kan denne lämna in klagomål till datainspektionen. De fattar då beslut ifall en översyn skall ske av det misstänkta företaget (Datainspektionen, 2018b). Ifall det finns ytterligare skäl, t.ex. att person lidit skada av den felaktiga behandlingen av personuppgifterna eller att dennes uppgifter har läckts kan person rikta skadestånd gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet (Datainspektionen, 2017f).

2.3.7 Personuppgifter och känsliga personuppgifter

Persondata som lagras kan huvudsakligen delas in i två kategorier, vanlig och känsliga persondata. Vanlig information kan t.ex. vara namn och liknande medans känsliga data räknas som sådan ifall man kan härröra följande från informationen: ”ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska åsikter, fackliga tillhörigheter och behandling av genetiska data” (Papakonstantinou & de Hert, 2016). Det som tillkommer i GDPR är biometrisk data och sexuell orientering. Denna känsliga data är förbjudena att processera såvida inte det finns särskilda skäl, som i allmänhetens intresse eller i medicinska syften.

2.3.8 Privacy by design

Privacy by design (PbD) är ett centralt koncept inom GDPR. Det går ut på följande (Multisoft, 2018):

- Samla in så få uppgifter som möjligt
- Lagra uppgifterna kortaste möjliga tid
- Åtkomststyrning till information dit minsta möjliga antal användare skall ha tillgång
- Uppgifter som samlas in skall skyddas under hela dess livslängd

Det är något som skall genomsyra allt arbete som hamnar inom GDPR:s svär, alltså hantering av personuppgifter och det gäller även mjukvara och liknande som utvecklas.

2.3.9 Backuper och GDPR

I dataskyddsförordningen, artikel 32 anges vad som gäller i samband med behandling av data. Bland annat nämns ”förmågan att återställa tillgängligheten och tillgång till personuppgifter i rimlig tid vid en fysisk eller teknisk incident” (Datainspektionen, 2018c), därmed underförstått att man skall ha backuper tillgängliga för den data som skall lagras. Dock nämns inget hur man skall göra med backuper ifall någon vill nyttja sin rätt att bli bortglömd/raderad (finns inget sätt att redigera backuper bakåt i tiden, finns media som bara går att skriva till osv, access till band osv).

2.3.10 Rutiner

Inför införande av GDPR kommer detta innefatta att rutiner måste finnas dokumenterade för både backuper och rutiner vid borttagning av personer, detta då verksamheten måste kunna påvisa vad som sker med den data som behandlas (Beckett, 2017). Detta kan innebära ett stort arbete för många företag då dokumentation ofta är något som faller mellan stolarna, t.ex. hos systemadministratörer som ansvarar för backuptagning och liknande (Limoncelli, Hogan, & Chalup, 2007).

2.4 Backup

I dagens IT-samhälle lagras mycket information i molnet eller på olika former av nätverkslagring. Denna lagring används av anställda eller privatpersoner för att lagra bilder, dokument eller viktiga handlingar och nästan all form av lagring i dag sker digitalt, alltså på någon form av disk någonstans.

Då diskar och lagring kan gå sönder har man sedan flera år tillbaka använt sig av backuper, dessa kan lagras på band eller på hårddiskar som sedan går in i arkivförvaring (Katayama, Chinda, Shimizu, Mikami, Suzuki, & Noguchi, 2016) eller roteras de och skrivs över efter ett tag. Utöver detta används backuper vid återställning av enskilda filer som användare råkat ta bort, eller som blivit korrupta. De flesta verksamheter har idag interna krav på att backuper skall finnas. Vid privat användning är det dock inte lika vanligt med backuper, annat än om man sparar i molnet eller har någon form av systemåterställning aktiverad i operativsystemet.

Backuper kom till av ett antal anledningar, bland annat för att begränsa skador som sker samt potentiella lagliga krav att spara specifik information (Limoncelli, et al. 2007), t.ex. högskolor och olika statliga organisationer måste ha viss data sparad. Ett exempel på detta är Skatteverket som måste spara inkomstdata om olika personer för att kunna kontrollera att rätt skatt dragits. Då informationen som lagras här är känslig och viktig krävs alltså säkerhetskopior på informationen. Det

som ofta föranleder en backup-plan är en riskanalys för att identifiera vilken data som behöver skyddas, därefter sätts en lämplig tidsplan upp för att ha data sparad så länge som kan anses behövligt inom verksamheten.

Dagens verksamheter har en stor mängd data om både kunder och anställda som sparas i olika applikationer och databaser. De är ofta inkluderade i backuperna då detta ofta är affärskritiska system, utan kunddata: inga ”deals”. Därför är backuper en väldigt central del i dagens IT-centrerade samhälle där allting handlar om att ha tillgång till rätt data vid rätt tidpunkt för att kunna genomföra sina affärer och verksamhetsplaner. I de fall backuper saknas leder detta ofta till stora ekonomiska förluster, dels förlorad arbetstid för att försöka återställa data och den tid man är utan sin kunddata. Ett exempel är när Pivab AB lejt ut sin drift av IT till ett annat företag, dessa saknade backuper på kundens data vilket ledde till att företaget förlorade sin företagsdata samt dryga böter för IT-företaget (Djurberg, 2018). Ett exempel kan vara att man förlorar all sin faktureringsdata vilket gör att man ej kan debitera sina kunder, därigenom ej få in de pengar man behöver för att driva verksamheten och betala löner.

Då dagens backuper är relativt oreglerade och det ej har funnits några större styrningar kring hur backuper skall hanteras eller vilken data som lagras på backuper har dessa kunnat sparas en obestämd tid, så länge företaget har behov av att ha kvar informationen. Alternativt tills dess att ett aktivt beslut tas att ta bort data. Detta innebär att beroende på hur backuprutinerna ser ut kan de registrerades information finnas kvar i all oändlighet hos företag, oavsett antal gånger de har interagerat med företaget i fråga. Offentliga organisationer berörs dock inte på samma sätt av detta. De behöver följa arkivlagen. Den anger vad som gäller för offentliga organisationer om t.ex. vad som behövs tas bort och vad som skall lagras (Arkivnämnden, 2018).

2.4.1 Backupmetoder

I dagsläget finns det huvudsakligen två olika metoder att genomföra backuper på. Det ena är fullbackuper, detta är vanligtvis en säkerhetskopiering utav samtliga filer på en partition medans den andra metoden är en inkrementell backup (Limoncelli, et al. 2007). Den sistnämnda metoden går ut på att enbart den information som ändrats sedan den sista säkerhetskopiering gjordes säkerhetskopieras, detta resulterar ofta i mindre backuper men däremot är de beroende av en obruten ”kedja” av inkrementella backuper för att kunna återställa bakåt i tiden. Fullbackuper tar å andra sidan stor plats då en sådan säkerhetskopierar all information på en disk, detta kan dock avhjälpas till viss del med hjälp av komprimering vid säkerhetskopieringen. Detta resulterar i att säkerhetskopian tar mindre plats än originalet, dock kan detta variera beroende på vilken applikation som körs.

Då säkerhetskopierna tar mycket plats (beroende på schema och typ) finns det huvudsakligen två aktuella medier att lagra dessa säkerhetskopier på. Det är hårddiskar eller på band. Band är det äldre mediet av de två men kan å andra sidan rymma stora mängder diskutrymme. Band är en relativt billig metod sett till mediet i sig självt, samt att det kan skrivas över vilket tillåter använding utav banden flera gånger, alternativt kan de vara engångsskrivbara och anpassade för arkivförvaring (Limoncelli, et al. 2007). När säkerhetskopiering sker fungerar det genom att en konstant ström av data skrivs till bandet och lagras i magnetiska strömmar. Dessa behöver matas konstant med data från t.ex. ett lagringskluster för att det skall hålla en jämn takt vid skrivning.

Det negativa med band är denna teknik ofta är väldigt kostsam vad det gäller utrustning kring banden för att genomföra backuperna, t.ex. läsaren och systemet för att styra skrivning osv, utöver detta är tekniken även långsam vad det gäller åtkomst till den information som lagrats på banden. Detta kan jämföras med hårddiskar, de var i början väldigt dyra och relativt lite utrymme fanns att tillgå, med tiden växte mängden data man kunde lagra på de roterande diskarna och det blev billigare att tillverka diskarna, därmed blev hårddiskar aktuellt som lagringsmedia för säkerhetskopiering. De brukar idag placeras i stora chassin där flera hundra terrabyte hårddiskutrymme kan erbjudas, på grund av sina växlande karaktär hos en hårddisk som erbjuder snabbare läs och skriv-hastigheter jämfört med band, där man skriver eller läser. Därför lämpar sig ofta hårddiskar bättre för upprepade backuper eller som mellanlagring för arkivförvaring, t.ex. redo för att skrivas till band. Utöver detta alternativ finns även Solid State Drives (SSD) som är flashminnes-baserade hårddiskar som erbjuder snabbare åtkomst till information pga. elektrisk åtkomst till informationen och bättre hållbarhet pga. avssaknad av rörliga delar. SSD:er lämpar sig väl till att lagra information och erbjuder även tekniker för snabbare radering av information genom funktioner som t.ex. ”trim” som är en funktion som används av SSD:er för att skriva över eller radera block av information som inte används längre (Data recovery, 2017).

2.4.2 Vilken data säkerhetskopieras?

Den information som organisationer vill säkerhetskopiera är ofta den som är affärskritisk. Detta kan vara allt ifrån databaser och den information anställda sparar på centralt administrerade lagringsresurser. Databaser är ofta en stor del i organisationer idag och informationen kan lagras på många sätt i dessa. Ett projekt som genomförts med syfte att se till att balansera tillgång till data mellan regulatorer, personuppgiftsbiträden och personuppgiftsägare hanterar intressanta sätt att dela på data. ”Meeting Upcoming GDPR Requirements While Maximizing the Full Value of Data Analytics” (Hintze & LaFever, 2017) tar upp detta genom att psydonomisera data som nämns explicit i GDPR och SOU 2017:39 (2017). Detta kan då skapa en säkrare databas och på detta sätt omöjliggöra åtkomst till data utan att ha rätt nycklar eller rätt behörighet för att koppla samman den lagrade informationen. Detta syftar då till att säkra personuppgiftsägares uppgifter genom att erbjuda ett fullgott skydd där ingen data kan kopplas till personen direkt. Om data lagras på detta sätt uteslutande skulle inget problem finnas, då ingen data är kopplad direkt till en enskild person utan enbart en entitet, detta möjliggörs genom sk. ”Kontrollerad länkbar data” (*Eng. Controlled Linkable Data”*). Detta tillsammans med säkerhetskopieringar på de enskilda delarna skulle kunna lösa viss problematik med att data går att återskapa och åter härleda till personer.

Ett annat arbete som direkt relaterar till obfuskering och anonymisering av information som lagras är ”A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation” (Bieker, Friedewald, Hansen, Obersteller, & Rost, 2016). Det som huvudsakligen hanteras i detta arbete är att ta fram en process för när och hur man skall genomföra en konsekvensbedömning av dataskydd samt hur man bör tänka kring den data som behandlas och därigenom genomföra förändringar för att skydda datan på bästa sätt.

Ett europeiskt projekt, ”Cloud accountability project” (Moe, Jaatun , Haugset, Niezen, Felici, 2013) genomfördes för att i samråd med olika tjänsteleverantörer komma fram till vad man skall kunna förvänta sig av GDPR och olika molnleverantörer (*Eng. Cloud Service Provider, CSP*). Det huvudsakliga ämnet som diskuterades i detta projekt var framförallt ansvaret hos CSP:s när det kom till hur data skall behandlas och lagras. De tar bland annat upp vilka aktörer som har vilket ansvar i vilken process

och till exempel hur ansvaret skall försäkras. Ett exempel är att CSP:en skall tillgodose att kunden har tillgång till dataklassificeringsverktyg för olika klassificeringar av data som lagras i molnet (hemligt, icke hemlig) (Moe, et al. 2013).

2.4.3 Redigering av backuper?

I dagsläget finns det inget stöd bland den mjukvara som används för backuper för att redigera dessa. Detta då grundtanken med säkerhetskopieringar länge har varit att dessa skall vara exakta kopior utav data vid ett fungerande tillfälle, redigering av backuper hade kunnat vara en lösning för att t.ex. radera registrerade med avseende på RABB.

Politou, Alpeis, & Patsakis (2017) tar i sitt arbete upp många av de problem som kommer med införande av GDPR med fokus på RABB och tillbakadragandet av sitt samtycke till datainsamlare. De behandlar även hur man på olika fronter har försökt lösa dessa problem genom olika implementationer av lösningar för t.ex rätten att dra tillbaka sitt medgivande genom t.ex. automatiserade metoder för anonymisering utav data i stora databaser som genomför automatisk profilering. Utöver detta tar de även med just problematiken med backuper och rätten att bli bortglömd, detta då lagen i deras mening säger att man måste bli borttagen i samtliga backuper också (Politou, et al. 2017). Men de lyfter då även fram den ekonomiska och arbetsmässiga bördan det faktiskt skulle innebära att genomföra detta, de ser framförallt att denna problematik kan komma att träffa finansiella institutioner, detta då dessa har en mängd olika krav på sig med avseende på att lagra transaktioner och liknande för spårbarhet.

Då säkerhetskopiering idag är kritiska för många verksamheter för att lagra t.ex. transaktioner och kunddatabaser behövs backuper, men samtidigt säger olika arbeten olika gällande rätten att bli glömd och backuper, ett exempel på detta är arbetet Brink, Elvland & Hansson (2017)där en av de som intervjuas tar upp just problematiken med hur man skall lösa säkerhetskopieringen, där det enligt henne inte finns något egentligt ”korrekt” sätt att genomföra borttagning av personer i backuperna utan att bryta mot den lagstiftning som GDPR anger. Därför bör företag idag ha genomfört eller påbörjat olika förändringar och anpassningar i sina verksamheter för att hitta ”sin” lösning på detta problem.

3 Problembeskrivning

Följande del kommer behandla det problem som författaren anser finnas tillsammans med frågeställningen, avgränsning, förväntat resultat och slutligen syftet med detta arbete.

3.1 Utmaningar med GDPR och backuper

Med GDPR kommer stora begränsningar och inskränkningar i hur företag faktiskt får behandla och delar personers uppgifter. Lagen anger vad som gäller med långtidslagring av data, vilket är under den tid det finns en laglig grund och behov av informationen. Den behandlar dock aldrig vad som gäller med specifika data som långtidslagras i backuper.

Den utmaning som framträder efter samtal med olika verksamheter är att väldigt många inte riktigt vet hur de ska förhålla sig till GDPR. Vissa har inte anpassat sin datalagring på något sätt medans några enbart lagrar backuper för en kort tid tillbaka. I många fall finns backuper på databaser och filservrar. Dessa kan innehålla blandad data som är strukturerad i databaser, ostrukterad i form av lösa filer med namn i löpande text och personnummer i olika dokument som t.ex. CV:n. Behövs inte den data som finns lagrad skall den tas bort enligt Datainspektionen (2018 F), men hur skall de göra om personen jobbade mellan 2008-2011? Skall de ta bort alla backuper där emellan eller skall de föra ett register över vilka personer som blivit borttagna som föreslås i intervjun i Brink, Elvland, & Hansson (2017) rapport?

Det kommer många frågetecken när dessa frågeställningar ställs, då GDPR även säger att backuper skall tas efter tolkning av artikel 32, del C där de säger att verksamheter skall inneha följande: ” förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,” (Datainspektionen, 2018e). Samtidigt säger lagen att data maximalt får lagras den längd som det faktiskt behövs, vilket lätt kan resultera att ens data finns kvar i arkivförvaring av backuper.

Något som Brink, Elvland, & Hansson (2017) lyfter fram i en av sina intervjuer är att backuper och hur dessa skall hanteras är under utredning, men att arbetsbördan för att faktiskt gå igenom backuper och ta bort data som rör personer är orimlig. De lyfter en lösning om att föra ett register över personer som vill bli borttagna, men då bör man per definition bryta mot GDPR redan då. Detta då man lagrar data om vem som vill bli borttagen.
De lyfter även en alternativ väg att gå, ifall begränsad backuptagning finns för kortare perioder. Lösningen skulle då vara att helt enkelt låta backuperna skriva över varandra, men då bryter man mot förordningens bestämmelser även där (Brink, Elvland, & Hansson, 2017).

Får man då enbart lagra datan i ett år eller vad är rimligt? Eller är det att man enbart får lagra backuperna så lång tid att dessa kan skrivas över med tiden, ifall en raderings-förfrågan inkommer?

3.2 Rutiner

Då en stor del i GDPR handlar om dokumentation och rutiner, något som systemadministratörer brukar dra sig för (Limoncelli, et al.2007) är detta något som alla bolag måste genomföra inför GDPR. Framförallt då det kommer finnas grund för inspektioner från datainspektionen och ett större arbete kommer ske med att faktiskt se till att företag efterlever GDPR. Att få fram rutiner som gör sig rätt

gentemot lagen är i många fall svårt, eftersom systemadministratörer är ofta inte jurister eller liknande. Därför får ofta extern hjälp anlitas i samband med detta.

3.3 Frågeställning

Den frågeställning som denna problematik mynnar ner i är följande och huvudfrågan i detta arbete är följande:

Hur har mjukvaruutvecklingsföretag valt att anpassa sin backuptagning med tekniska och rutinmässiga förändringar inför GDPR samt vad har de för rutin gällande rätten att bli glömd?

Problemet i sig är att det i dagsläget inte finns några tekniker för att redigera och radera enskild information i backuper, utan antingen får man ta bort backupen eller undvika att återställa till backuper ifall en registrerad vill bli borttagen. Utöver detta ligger det i backupers natur att man inte vill ändra i dessa, för att backupers syfte är just att vara en ögonblicksbild över hur informationen såg ut där och då.

Samtidigt i och med att GDPR är nytt, finns inga prejudikat eller riktlinjer kring hur verksamheter skall anpassa sina säkerhetskopieringsrutiner utan enbart lagtexten som säger att backuper skall finnas med samtidigt skall man kunna tas bort ur samtliga data som finns om man begär det.

Delmål

I huvudfrågan finns ett antal delfrågor som kommer leda till att huvudfrågan kan besvaras.

1. På vilket sätt har verksamheterna förändrat sin rutin för säkerhetskopiering?
2. Hur har verksamheterna utformat sin rutin för ifall någon vill bli bortglömd med avseende på backuper?
3. Hur har verksamheterna rent tekniskt förändrat säkerhetskopiering av informationen?
4. Hur ser verksamheterna på framtiden vad gäller säkerhetskopiering, rätten att bli glömd och GDPR?

3.4 Syfte

Arbetet ämnar ge en antydan kring hur mjukvaruutvecklingsföretag har valt att anpassa sig efter den nya lagstiftningen, samt vad de har gjort för att anse sig förberedda inför GDPR och den problematik som kommer med den för verksamheter och systemadministratör.

Detta arbete kan nyttjas av organisationer eller företag som vill ha möjlighet att läsa hur andra företag valt att anpassa sig inför den nya lagstiftningen samt nya sätt att tänka kring hur man kan hantera de rutiner som man behöver inför GDPR. Utöver detta kan även arbetet användas för att se vilka svårigheter företag haft i samband med implementeringen av sina förändringar eller varför de har avstått från att genomföra förändringar inför GDPR.

Utöver detta finns det ej något tidigare arbete som undersöker denna verksamhetskritiska del och specifika del kring GDPR och verksamheters anpassning inför den. Därför kan detta arbete vara till stor nytta för de företag som driver sin egna IT och administratörer runt om i landet som ställer sig

frågande till den nya lagstiftningen, samt hur de skall hantera den inom sin verksamhet med avseende på rutiner och backuper samt rätten att bli glömd.

3.3 Avgränsning

På grund av studiens tidsram och omfång har en avgränsning gjorts i arbetet genom att fokusera på de tekniska lösningar och de rutiner som verksamheter har implementerat. Backupmetoder och hur verksamheter bör förhålla sig till GDPR och tips inför detta finns det gott om arbeten kring, men ej specifikt något som undersökt hur företag har anpassat sina backuper, tekniskt och rutinmässigt inför införandet. En avgränsning har även valts att göras i vilket geografiskt område intervjuerna kommer genomföras och dessa kommer hållas till ett område kring Skövde för att kunna genomföra intervjuerna effektivt.

3.4 Förväntat resultat

Med tanke på de implikationer och sanktioner som GDPR medför vid överträdelser och de strikta regler som gäller får de antas att verksamheter gjort vissa förändringar, åtminstone vad det gäller rutiner. Hypotesen är sådan att verksamheterna kommer ha genomfört vissa förändringar, bland annat infört rutiner vad gäller borttagning av personer. Dock kommer förmodligen de flesta företag ej genomfört några större förändringar rent tekniskt på sina backuper eller ändrat några rutiner vad gäller detta. Detta grundar sig i de krav som finns på att rutiner och dokumentation skall finnas kring hur och var informationen finns och hur den behandlas.

Detta är väldigt situationsbaserat om detta är bra eller dåligt, vissa företag kanske redan tar backuper och lagrar maximalt en månad, medans vissa företag lagrar data för minst ett år tillbaka. Då det är relativt tidsbegränsat arbete innebär detta att man ej kommer kunna djupdyka inom flera enskilda företag, utan istället kommer det bli mer generellt men ändå fokuserat på de delar som detta arbete ämnar ge svar på.

4 Metod

Följande del kommer behandla den metod som kommer nyttjas för att finna svar på den problematik denna rapport lyfter fram. Inledningsvis kommer metodvalet att behandlas för att därefter gå in på utformningen av intervjun och det som hör där till. Efter metoden kommer validiteten tas upp följt av en del som behandlar etiken i denna rapport. När dessa delar behandlats kommer urval, metodsteg, genomförande och tillförlitlighet och genomförbarhet att behandlas.

För att studien skall hålla en god kvalité nämner Berndtsson, Hansson, Olsson, & Lundell (2008) vikten av rätt metod samt teknik väljs för att säkerställa ett gott resultat ifrån arbete. Därför kommer de olika metoderna att förklaras och motiveras varför dessa passar bra eller mindre bra i syftet att besvara frågeställningen.

4.1 Val av metod

Det finns många vägar att gå för att besvara en forskningsfråga, men alla är inte lämpade för att besvara vissa frågor. Berndtsson, et al (2008) nämner metoder som litteraturanalys, intervjuer, fallstudier, enkätundersökningar och experiment.

Då rapporten syftar till att besvara hur företagen faktiskt har förändrat sitt arbete (om detta gjorts), är någon form av direkt kontakt med företagen att föredra. Detta antingen genom enkäter eller intervjuer. Detta lämpar sig väl då man kan få direkt korrespondans med företagen och få deras ansvarigas personers svar på hur sakerna gjorts.

Då detta är ett relativt outforskat ämne med ett specifikt fokus, finns det ej mycket tidigare arbete att gå på. Därför faller även en litteraturstudie bort i detta fallet.

Enligt Berndtsson, et al. (2008) används ofta kvalitativa studier i sociala sammanhang för att skapa en förståelse för varför saker är som de är och inte försöka förklara tillstånden. Då detta stämmer väl överrens med denna studies inriktning faller ett experiment bort direkt från ett av de möjliga alternativen, och kvar står en intervjuer eller fallstudier. Anledningen till att enkätundersökningen faller bort är att denna metod räknas som kvantitativ och därför inte kan ge den exakthet eller mängd information som efterfrågas på ett adekvat sätt. Detta då undersökningarna skulle vara för stora för detta arbetets omfång med den frågeställning som finns.

Wohlin (2012) nämner t.ex. om fallstudier att dessa ofta används när ämnena inte kan undersökas isolerat, vilket så är fall när arbetet ämnar kontrollera vad företagen har gjorts och inte gjort. Detta är något som måste ske hos företagen, med personer som kan svara på detta. Därför faller valet av metod i detta arbete på kvalitativa intervjuer då det faller utanför detta arbetes avgränsing att kontrollera hos enskilt företag hur dessa anpassat sig i en fallstudie.

4.2 Intervjustudie

Fördelarna med en intervjustudie är enligt Flick (2013) ”*you can study subjective viewpoints in different social groups*”, detta lämpar sig väl i denna rapport då den syftar till att undersöka hur olika företag valt att anpassa sig inför samma problem. Utöver detta nämner Flick (2013) även att denna metod lämpar sig väl för att skapa sig en djupare förståelse av de saker som undersöks.

En intervjustudie syftar till att få svar från de tillfrågade på de forskningsfrågor som ställs i rapporten. Dessa skall dock inte ställas direkt (Wohlin, 2012) utan anpassas för att ge en bredare bild som sedan kan analyseras och ge svar på den frågeställning som ges. Under intervjuerna kan frågorna som ställs vara öppna eller stängda, öppna frågor ger den som svarar stor frihet och kan därför lätt hamna ur fokus. Stängda intervjuer kan användas för att limitera den intervjuades svarsalternativ, genom t.ex. ja eller nej frågor eller kortfattade svar.

Då det inte är särskilt givande att kontrollera hur ett företag har förändrat sig inför GDPR är fokuset i denna rapport på flera företag. Dessa kommer hållas till sex företag för att få en god grund, antalet begränsas på grund av svårigheter med att få företag att ställa upp samt att det som undersöks är detaljerat i sitt ämne (Hedin & Martin, 2011).

4.3 Övergripande literaturgranskning

För att kunna genomföra detta arbete har en grundläggande inläsning behövt ske för att förstå GDPR och hur företag har hanterat sina backuper tidigare. Detta har genomförts för att på ett korrekt sätt kunna ställa frågor till företagen och för att skapa en förståelse kring vilka problem företagen möter inför GDPR. För att förstå vilka problem som uppkommer i samband med GDPR och backuper har en inläsning gjorts på de problem som företag kommer ställas inför, något som bland annat Politou, et al. (2017) tar upp i sitt arbete.

Huvuddelen av källorna i detta projekt har inhämtats via olika vetenskapliga databaser, exempel på detta är t.ex. Springer, IEEE Xplore och DiVA samt Google scholar. För att få fram de resultat som har nyttjats i rapporten har sökord som ”GDPR and backups”, ”GDPR” och ”GDPR the right to be forgotten” använts. De arbeten som har valts ut ifrån dessa sökningar har varit arbeten med en god kvalité enligt den bedömningsmodellen som är framtagen vid högskolan.

4.4 Frågekonstruktion

Enligt Wohlin (2012) finns det huvudsakligen tre olika metoder att nyttja sig av vid en intervjustudie, dessa är ostrukturerade, semi-strukturerade och hel-strukturerade. I ostrukturerade intervjuer är oftast frågorna väldigt generella och öppna, desas syftar till att hålla en öppen intervju som inte planeras, utan dessa hålls öppna där den intervjuade talar fritt och den som intervjuar anpassar frågorna efter hur intervjun fortgår (Berndtsson, et al. 2008) .

I en semikonstruerad intervju kombineras ofta öppna och stängda frågor, dessa kan då ofta användas som en öppen fråga tillsammans med en stängd konfrontativ frågeställning (Flick, 2013). I dessa fall används ofta frågeguiden mer som en checklista än ett manus och tillåter därmed den som interjvuar att anpassa intervjun med frågeställningar beroende på vad man talar om. Detta stärks även utav Bryman (2018) som anser att öppna frågor lämpar sig väl för nya områden och man kan även fånga upp ovanligheter i svar och liknande.

Den metod som valdes i detta fall är en semikonstruerad intervju för att tillåta större frihet i genomförandet i intervjun, och samtidigt se till att hålla intervjun till ämnet. Intervjun kommer utformas enligt de fyra steg som Wohlin (2012) nämner, inledningsvis kommer målen med intervjun och arbetet att presenteras samt hur den kommer bli använd. Därefter kommer några frågor ställas kring personen som blir intervjuad för att därefter övergå i den faktiska intervjun. Frågorna som ställs

i huvudintervjun baseras på de frågeställningar som denna rapport ämnar svara på tillsammans med de problem som Politou, et al. (2017) lyfter i sin rapport.

4.5 Validitet

För att säkerställa en god validitet i rapporten och dess resultat nämner Kvale (1997) sju stadier, tematisering, planering, intervju, utskrift, analys, validering och rapportering. Dessa skall appliceras genom hela arbetsprocessen med denna rapport och om samtliga uppfylls, t.ex. angående valet av personer att intervjua och dess tillförlitlighet som intervjuade ökar arbetes kvalité och validitet.

På de arbeten som används som grundkällor i detta arbete genomförs en noggrann och kritisk granskning kring hur dessa kan anses rimliga och vilka källor dessa nyttjat sig av. Detta för att utesluta eventuella validitetshot mot detta arbete ifall deras blir ifrågasatt. Utöver detta itereras dessa arbeten igenom för att återigen säkerställa deras relevans gentemot arbetet som genomförs.

Utöver detta är även ett hot mot det egna arbetet att forskningsfrågan inte får något svar. Detta förefaller vara ett mindre hot men ändå nämnvärd, men då flera företag kommer att intervjuas kommer en generell bild att kunna byggas upp, men om inget företag skulle ställa upp skulle detta självklart falla. Ett annat validitetshot som kan påverka rapporten är valet av metod, då detta föll på att genomföra en intervjustudie finns vissa validitetshot om egen partiskhet (Berndtsson, et al. 2008) samt att man kan påverka de man kommer intervjua. Viss partiskhet kommer alltid finnas då den som genomför arbetet har bildat sig en uppfattning kring ämnet samt även de tillfrågade. Dock genom att vara medveten om detta kan man aktivit försöka motverka detta och försöka bibehålla en neutral ställning till ämnet.

Gällande valditetshot mot metodvalet i sig är detta framförallt att resultatet kan bli svårt att generalisera, detta då antalet företag som undersöks är begränsat. Men detta valditetshot hanteras till viss del då frågorna kommer vara generella och genom ett strikt urval av personer och företag inom en specifik sektor och avgränsat område, på detta sätt kan fyllnad i svaren uppnås (Kvale & Brinkmann, 2014).

4.6 Etik

Under arbetes gång har Kvale (1997) tablå om etiska frågor i de sju forskningsstadierna följts, detta är något som genomsyrar allt. Etik är viktigt, speciellt i avseende där forskning sker med människor som deltagare, enligt Kvale (1997) ”forskning med människor som deltagare måste tjäna vetenskapliga och mänskliga intressen”.

Något som är centralt både inom GPDR och etiskt arbete är att allting sker med hjälp av samtycke och klara förutsättningar. Därför informeras de intervjuade tydligt om arbetets syfte och att de när som helst kan återkalla sitt samtycke till deltagande i studien. Utöver detta är även konfidentialitet en viktig punkt, detta då de intervjuade skall ha möjlighet att välja om deras namn och liknande som kan användas för att identifiera de eller deras företag. På grund av att backuper och rutiner kring dessa kan vara ett känsligt ämne hos vissa företag kommer därför samtliga inhämtade data att anonymiseras redan vid transkribering, detta för att undvika eventuell identifiering utav person eller företag, detta beror på att enligt Kvale (1997) skall risken för skada mot undersökningsperson vara så liten som möjligt, eller i detta fallet ett företag. Något som däremot är relevant för studien i sig är inom vilken sektor företagen verkar, därför kommer sektor att finnas med. Under själva intervjuerna

kommer den som intervjuar behöva vara lyhörd och aktivt verka för att förstå och tolka den intervjuade korrekt. Utöver detta skall man även undvika att påverka den intervjuade under intervjun. Samt, den som intervjuar har stort ansvar i att data är riktig Kvale (1997). Detta säkerställs genom att inhämta godkännande från respondenterna efter transkribering för att ge de en chans att rätta potentiella missförstånd eller felaktigheter i intervjun.

4.7 Urval

De personer som skulle vara aktuella för intervjuerna skulle vara personer som jobbar med IT på varierande företag som handhar sin egna IT-miljö, dvs. att de själva bestämmer när t.ex. backuper tas, hur de tas och hur länge de lagras. Utöver detta skall personerna även inneha ledarroller inom det bolag de verkar inom.

Detta urval baserar sig på Patton (2015) som benämner detta som *"purposeful sampling"* som syftar till att förväg försäkra sig om att personerna som blir tillfrågade innehar den nödvändiga kunskapen kring lagen och de ämnen som undersöks.

De företag som intervjuas skall utöver ovan nämnda kriterier även vara företag som handhar persondata i sina system och har ansvar för hur denne hanteras. Utöver detta skall företagen verka inom utvecklingsbranschen med avseende på mjukvaruutveckling. Valet att inrikta sig på mjukvaruföretag är p.ga. dessa upplevs av mig hamnat i skymundan vad gäller GDPR och diskussionerna kring detta och även den täthet av mjukvaruutvecklingsföretag som Skövde och dess närhet innehar.

Dessa intervjuer skall godkännas av personerna som blir intervjuade för att ta hänsyn till vetenskapsrådets forskningssed (kap4.4) Utöver detta då detta kan anses vara företagskritiska system och för att ej undanröja deras rutiner kommer alla företagsnamn och personer att förbli anonyma, utan enbart inom vilken sektor dessa verkar inom (Vetenskapsrådet, 2017).

4.8 Metodsteg

Genom att fastställa vilka steg studien skall följa och se till att de uppsatta målen klaras av har följande metodsteg satts. Dessa genomgås i kronologisk ordning och representerar olika delar som skall klaras av innan nästa steg påbörjas:

1. Inledningsvis sker en inläsning på ämnet. Detta för att skapa en förståelse kring det ämne som rapporten kommer behandla. I denna del genomförs även bakgrunden och problemformuleringen.

2. I detta steg väljs metoden baserat på vad som kan anses vara mest lämpligt för genomförande av studien. I detta steg genomförs även en analys av validitetshot och genom arbetet betänks validiteten i de källor som nyttjas och hur allt påverkar arbetet. Utöver detta betänks även etiken i arbetet och hur man skall anpassa arbetet efter gällande etiska riktlinjer.

3. I detta steg genomförs frågekonstruktionen och även intervjuerna i sig. Detta för att kunna samla in data och analysera data. Här ingår även transkriberingen utav det insamlade materialet som härrör från intervjuerna.

4. I det sista steget sker analysen utav det insamlade materialen. Detta syftar då till att slutligen kunna besvara den forskningsfråga som ställs. I slutändan dras slutsatser och en diskussion kring arbetet sker samt hur man skulle kunna fortsätta framtida arbete på detta.

4.9 Genomförande

Inledningsvis fastställs att studien kommer genomföras anonymt. Detta då backuper för de tillfrågade verksamheterna är en känslig fråga. Utöver detta kommer studien att ske genom olika former av kommunikationsmedel, vissa utav intervjuerna kommer att genomföras hos företagen, detta då de anställda då kan känna sig mer trygga i den miljö de befinner sig i. Detta tillåter då den intervjuande att samla in den visuella information och atmosfären under intervjun (Kvale, 1997) vilket till viss del kan vara subjektiv enligt vissa. Vissa utav intervjuerna bedrivs via applikationen Skype. Skype är att föredra då man på detta sätt enkelt kan återspegla den intervjuades kroppsspråk som kan vara viktigt vid transkriberingen, dock kommer enbart ljudet spelas in. Video används under intervjun då man ej kan uppfattade den intervjuade på plats vilket tillåter en att se på intervjun och samla in de uttryck som ges samtidigt som intervjun genomförs. Utöver detta, enligt Bryman (2018) finns det vissa belägg för att skillnaderna mellan en intervju via telefon och ansikte-mot ansikte enbart är ringa.

Studien genomförs huvudsakligen med olika befattningshavare inom IT, dessa har varit med och tagit fram de rutiner som företaget nyttjar sig utav gällande backuper och även varit med och bestämt hur företag skall anpassa sig (om detta gjorts) inför GDPR.

4.10 Transkribering

När samtalen skall föras ner från ljud till text tillkommer en del aspekter som bör betänkas noggrant. Ett exempel på detta är t.ex. reliabiliteten (Kvale, 1997) , validiteten och etiken i det arbete som görs. Enligt Kvale (1997) är en tranksribering:” att göra en utskrift innebär att översätta från ett talspråk, med sin egen upssättning regler, till ett skriftspråk med en annan uppsättning regler.”

När det kommer till reliabilitet nämner Kvale (1997) bland annat att olika personer kan tolka en inspelning olika och därmed kommer slutresultatet skilja sig åt. Därför kommer enbart en person att tranksribera materialet och transkribering kommer ske med en ordagrann stil, detta för att kunna erbjuda exakt vad som sagts och få med pauser och liknande.

Gällande arbetes validietet vid transkribering kommer materialet transkriberas på ett ordagrant sätt, detta för att göra det mer komplett och erbjuda en direkt replikering av den intervju som genomförts för att därför kunna anylsera resultaten med vad som faktiskt sagts.

Etiken är något som bör tas i särskild beaktning när man genomför intervjuer, detta då dessa genomförs med andra människor som har egna tankar, värderingar och sätt att uttrycka sig. Utöver detta behandlar även intervjun känsliga ämnen inom verksamheterna då detta rör sig om just hur man föhåller sig till en lag som träder i kraft är det viktigt att värna om den intervjuades konfidentiallitet (Kvale, 1997). Därför kommer intervjun som transkriberas att anonymiseras för att inga namn eller möjlighet att härleda vilken verksamhet som blivit intervjuade framträder.

Det finns även några problem vid transkribering utav ljudinspelningar, dessa är bland annat att t.ex. sarkasm eller liknande kan vara svårt att tyda i inspelningar, dessa hade kunnat fångas med hjälpa av

en kamerainspelning men på grund av det känsliga ämnet och den konfidentialitet som präglar detta arbete valdes detta bort.

4.11 Analys

För att kunna analysera resultatet från den transkribering som skett kommer en tematisk analys att nyttjas. Denna metod är en av de vanligaste metoderna att angripa och analysera (Bryman, 2018) kvalitativa data. I denna metod delas olika delar av informationen in i olika teman, och det kan vara följande enligt Bryman (s. 703, 2018):

> ”- En kategori som identifierats av analytikern utifrån hans eller hennes data
> - Temat är kopplat till forskningen fokus (och sannolikt även till forskningsfrågorna
> -Det bygger på koder som identifierats i utskrifter och/eller fältanteckningar.
> - Det förser forskaren med en grund för en teoretisk förståelse av hans eller hennes data som kan utgöra ett teoretiskt bidrag till litteraturen på det aktuella området.”

För att analysera den information som samlats in kommer de olika temana att identifieras och därefter kommer de deltemana att identifieras i informationen, dessa kommer sedan att ställas upp i olika kolumner för varje deltema och därefter att jämföras och analyseras. Metoden kallas ”framework” (Bryman, 2018) och beskrivs som ”en matrisbaserad metod för att ordna och sammanställa data” (Bryman, 2018; Ritchie m.fl. 2003 s.219)
Vid skapandet av matrisen placeras då olika stycken från de transkriberade intervjuerna i de passande deltema-kolumnerna och därefter kan en jämförelse göras mellan de olika parternas svar, oftast används repetitioner för att identifiera de olika teman och delteman som finns.

5. Resultat

I följande del kommer en objektiv presentation av det som framkommit under intervjuerna att presenteras, inledningsvis sker en presentation av respondenterna och därefter en summering av resultatet från intervjuerna.

5.1 Presentation av verksamheterna och respondenterna

De olika verksamheterna som sökts upp har varit verksamheter som är utvecklande i sin art, de utvecklar och säljer alltså mjukvara som andra företag eller privatpersoner nyttjar till vardags.

Respondent 1

Verksamhet 1 är ett företag som utvecklar olika finansiella program för olika verksamheter för hantering av fakturor, inkasso och liknande. Respondenten hos detta företag i detta fall är Chief Operating Officer (COO) och har hand om den operationella driften av företag i vardagen samt är utsedd Data Protection Officer (Dataskyddsombud, DPO) vid verksamheten.

Respondent 2

Verksamhet 2 är även detta ett företag som fokuserar på att finansiella program för t.ex. transaktioner och beslut. Respondenten vid detta företag är IT-chef och har varit högst delaktig i införande av GDPR och satt rutiner vid verksamheten, framförallt inom de tekniska aspekterna.

Respondent 3

Verksamhet 3 är en verksamhet som specialiserar sig på finansiella program och fakturering för olika verksamheter och tillhandahåller mjukvara för att nyttja deras tjänster. Respondenten vid denna verksamhet är IT-ansvarig vid verksamheten och även DPO. Respondenten har varit delaktig i införandet och utvecklingen utav samtliga rutiner vid verksamheten gällande GDPR.

Respondent 4

Verksamhet 4 är en verksamhet som håller på med spelutveckling och säljer sina spel på den globala marknaden. Respondenten är systemadministratör och håller även på med utbildning inom verksamheten och programmerar. Respondenten har inte delaktig i utvecklingen av rutiner och liknande inför GDPR utan har varit ansvarig för att implementera de rutiner och det som behövs göras.

Respondent 5

Verksamhet 5 är en verksamhet som inriktar sig på administrativa programvaror. Respondenten jobbar som marknads- och försäljningschef vid verksamheten och har varit delaktig i införande av GDPR vid verksamheten, både vad gäller rutiner och arbetssätt.

5.2 Sammanfattning

I detta stycke kommer de olika respondenternas svar att ställas upp under de olika delmålen för att tydligt koppla an till den frågeställning som rapporten ämnar ge svar på.

5.2.1 På vilket sätt har verksamheterna förändrat sin rutin för säkerhetskopieringen?

Huvuddelen av de tillfrågade verksamheterna har ej genomfört några direkta förändringar kopplade till rutiner kring backuptagning och rutiner kring dessa. Respondent 1 svarar däremot att de kontinuerligt ser över sina rutiner kring backuptagning och hur denna skall anpassas kring olika lagar och regler. Det som nästan samtliga respondenter har gemensamt är att de har jobbat aktivt med att dokumentera de rutiner de har. Vissa av respondenterna valde även här att ej gå in på detaljer kring hur deras backuptagning och rutinen i sig ser ut, utan refererar då till företagshemligheter. Respondent 1 väljer även att lyfta fram deras uppdelning utav information som de genomfört, där enbart viss personal har tillgång till informationen som blivit säkerhetskopierad.

> *” Ja, på backup:er jobbar vi kontinuerlig med att förbättra och förändra oss och anpassa oss utifrån hur marknaden ser ut och hur lagkrav ser ut och hur vi kan jobba säkrare men vi jobbar ju i en förtroendebransch så att vi måste ha”*

Respondent 4 nämner att de ej genomfört några större ändringar i dokumentation kring deras förfaranden utan de anser istället att de ej behöver genomföra detta med grunden att de ej sparar några direkta personuppgifter.

Värt att nämna är även att flera av respondenterna har valt att förlägga sina backuper hos olika moln-leverantörer för en spridd risk och ökad tillgänglighet. Kopplat till GDPR har framförallt respondent 2 valt att kravställa gentemot sin leverantör att enbart företaget skall ha tillgång till nyckeln för att kunna låsa upp de säkerhetskopieringar som är gjorda.

Något som även är nämnvärt är att 2 av de tillfrågade respondenterna (2 och 3) enbart lagrar sina säkerhetskopior en kort tid, detta motiverar de då med varför de känner att de ej har några direkta krav att förändra sina rutiner kring säkerhetskopiering.

Något som respondent 2 lyfter fram är att man jobbar aktivt med att kunna återställa från sina säkerhetskopior, detta genom att simulera driftstörningar och systemkrascher. Det som de framförallt undersöker i detta fall är just hur de skall återställa sina kopior som de har lagrade hos sin tjänsteleverantör. När det kommer till just återställning och större krascher svarar samtliga respondenter att de aldrig behövt göra någon större återställning av maskiner utan detta har då rört sig om enskilda filer som tagits bort eller liknande.

Respondent 5 har ej heller genomfört några förändringar gällande sina backuper utan satt mer formella krav på att data inte kan lagras på obegränsad tid, även om kund begär det. Dock har de satt med i deras PUB-avtal att information om de registrerade gallras ur den aktiva miljön med jämna mellanrum som det sedan tas säkerhetskopior på.

5.2.2 Hur har verksamheterna utformat sin rutin för ifall någon vill bli bortglömd med avseende på backuper?

Något som är genomgående bland huvuddelen av respondenterna är att de har jobbat aktivt med rutiner och dokumentation kring hur de ska lösa de olika problem som de ställs inför med GDPR. Respondent 1,2,3 och 5 har fastställda rutiner för hur de skall gå tillväga och ett tänk kring detta.

Respondent 1 har valt att lösa detta genom att ej lagra någon kunddata aktivt utan att istället låta data som kommer in från kunder anonymiseras först innan den hanteras av någon anställd. Därför lagrar de ej några uppgifter kring kunderna annat än det som krävs för avtal och liknande. Gällande sina egna anställdas information kommer denna att hanteras och tas bort inom rimlig tid.

Respondent 2 och 3 som kan hantera persondata direkt genom deras system har valt att genomföra en lösning som bygger på att manuellt gå in i den aktiva information och radera personen ur denna. Respondent 3 nämner även att de har en process på gång för att automatiskt kunna radera personer vid förfrågningar. Respondent 2 och 3 nämner även detta att beroende på den mängd förfrågningar som de får in om att bli borttagna kommer de eventuellt också att automatisera processen för borttagning.

Respondent 4 har i för närvarande ingen rutin satt för borttagning av konton och liknande utan har istället valt att lösa det som det kommer. Detta är dock något som kommer in till supporten som hanterar detta istället. Det sker alltid i mån av tid och tillgängliga resurser vid tillfället.

Respondent 5 har en rutin satt där de kommer ta bort personen ur den informationen som finns lagrad just nu, detta sker efter en begäran från deras kund som är personuppgiftsansvarig Om en begäran kommer in anser de att en rimlig tid för borttagning är ca 2 veckor.

> *” det finns ju med i vårt PUB-avtal, hur länge vi kommer gallra om inget annat benämns i huvudavtalet så att säga, men det kan vi ju komma överens om, att gallra efter 180 dagar eller plocka bort allting eller hur vi ska göra, det kan man ju ställa”*

Med avseende på säkerhetskopieringar har respondent 2 och 3 valt liknande lösningar där de kommer ta bort en person och därefter låta backuperna rulla över varandra, detta då de enbart lagrar sina säkerhetskopior en kortare tid, respondent 2 lagrade de i 2–3 månader och respondent 3 lagrar dessa i maximalt 5 veckor innan dessa skrivs över. Respondent 5 svarade i detta fall att de lagrar sin data i upp till 5 år som standard då det kan vara av vikt att få fram gamla schemadata och vem som genomfört ändringar vid vilken tidpunkt. Respondent 1 valde här att yrka på företagshemligheter.

Rent rutinmässigt har verksamheterna dokumenterat vilken data som finns var och hur denna skall hanteras. Respondent 4 skiljer sig dock från mängden där de resonerar att de ej har några personuppgifter lagrade kring sina kunder förutom mejladresser och kontonamn, då allt hanteras av tredje part och enbart koppling finns till extern tjänst och deras konto där, därför har de ej gjort någon dokumentation eller satt upp en rutin vad det gäller att rätten att bli bortglömd.

Ingen respondent har i detta fall valt att aktivt ta bort backuper eller satt upp en rutin för att ändra data i de tidigare backuper som finns, utan de har valt att exkludera dessa från rutinen i sig vad gäller borttagning, detta då de anser att den insamlade informationen är ”vilande” och därför ej används

aktivt. Respondent 2 gick dock in på en alternativ lösning där de lyfte fram möjlighet till att byta nyckel på sina gamla backuper för att göra de oanvändbara och därmed oåterställningsbara för att skydda sin data från återställning vid borttagning.

Utöver ovan nämnda har respondent 1-3 samt 5 även sagt att de kommer informera personerna om att borttagning skett, de kommer i de fall meddela kunden om vad som tagits bort och vad de ej kan ta bort med avseende på andra lagar.

> *”Sen i backup:er, det faktum att det är krypterat, man kan säga om den krypteringsnyckeln byts då är de gamla backup:erna i princip värdelösa så vi behöver inte fysiskt radera då. Det är bara noise utan nyckel.”*

5.2.3 Hur har verksamheterna rent tekniskt förändrat säkerhetskopiering av datan?

Generellt har företagen ej gjort några förändringar kring tekniska lösningar kring sina backuper, samtliga företag krypterar sina backuper förutom respondent 4 där verksamheten valt att avvakta med detta. De skyddar istället sin data genom att den är spridd i multipla regioner och har en databas som enbart går att läsa ifrån som de tar backup ifrån. Utöver detta svarar även respondent 1 och 4 att de även skyddar sig genom att låta informationen replikeras mellan olika servrar, detta för att säkerställa att informationen finns på flera platser/servrar samtidigt.

> *” I ett initialt skede tas den backupen till en filserver i en annan region. Huvuddatabasen är egentligen i en region, om vi talar datacenter-mässigt, read only:n finns i ytterligare en annan så om det ena datacentret skulle sprängas så har vi backup så att säga medan backupen tas till ytterligare en tredje region”*

Genom att kryptera säkerhetskopiorna skyddar de alltså informationen. Respondent 2 och 5 svarar här att de är de enda som har tillgång till nyckeln, respondent 3 svarar här att de delar nyckeln med deras tjänsteleverantör som servrarna står hos. Respondent 2 nämner även möjligheten till att byta nyckel på de äldre säkerhetskopiorna för att göra de oåterställningsbara.

Huvuddelen av företagen har även här externa resurser som tar säkerhetskopior åt verksamheterna, detta rör sig alltså om respondent 2,3 och 4, detta genomförs då genom en s.k. ”hosting-provider” (tjänsteleverantör) där deras servrar då är placerade. Respondent 2 har en lösning där de har både en backup lokalt som sker genom replikering av maskinerna var 15:e minut och som sedan synkroniseras med en moln-leverantör för vidare lagring. Respondent 3 har valt att lösa säkerhetskopieringen genom att ta backuper lokalt på de filer som det jobbas med internt och låter tjänsteleverantören ta säkerhetskopior på den data som är i produktionssystemen.

Respondent 1 är den utav de tillfrågade verksamheter som antyds har skiftat lagring utav sina backuper, de har gått över till lagring utav backuperna till SSD:er för snabb access. De andra respondenterna har här valt att ej genomföra någon förändring gällande vilket lagringsmedium som nyttjas, utan nyttjar sig av de resurser som de haft i dagsläget hos sig och hos sin tjänsteleverantör. Respondent 5 är den verksamhet som i dagsläget har sin egna drift och serverhall och därför full kontroll över sin data, detta härstammar från olika krav som deras kunder ställer i hanteringen av personuppgifterna som lagras i deras system. Respondent 5 är den som hanterar känsligast uppgifter, detta då det inkluderar hantering utav barns uppgifter.

5.2.4 Hur ser verksamheterna på framtiden vad gäller säkerhetskopiering och rätten att bli glömd?

Huvuddelen av respondenterna anser att det är för tidigt att säga något specifikt, överlag anser de dock att man kommer få rätta sig allteftersom beroende på prejudikat och liknande som framkommer efter domstolsmål. Just angående säkerhetskopior tror respondenterna att detta kommer att vara som det är ett tag framåt, till dess att en dom kommer som kan ange vad som faktiskt gäller angående säkerhetskopior och rätten att bli glömd, detta då respondenterna överlag anser att säkerhetskopior är något som behövs för verksamheten och att det ej finns någon teknisk lösning för att modifiera säkerhetskopior i dagsläget.

> *" Jag tror nog att EU kommer vilja göra ett statuerligt exempel och slå ner på ett antal aktörer och då får vi se vad som händer helt enkelt.".*

Framgent tror respondenterna att ytterligare styrningar kommer att komma men inget specifikt utan enbart riktlinjer kring detta, detta då de anser att de ej kan detaljstyra datalagring på lagnivå. Något som däremot framträder under intevjuerna är att huvuddelen av respondenterna tror att de flesta företag kommer fortsätta jobba aktivt med GDPR och anpassningar som kommer. Respondent 3 tror dock att *" tyvärr att efter 25:e är det många företag som kommer att lägga ner det här arbetet eller ha extremt lite fokus på det och det kan visa sig farligt."* Respondent 1 visar däremot ett större förtroende för branschen och framtiden och säger:

> *"Jag tror att företag kommer fortsätta anpassa sig och jag tror att branscher säkert kommer komma med rekommendationer kring hur man skall göra. Så att det sanerar sig självt*"

Utöver detta nämner respondenten även att i samband med att Sverige har PUL bör därför vi ligga längre fram än många andra länder vad det gäller rättigheter och hur personuppgifter hanteras.

Angående kontroller och inspektioner som kan göras tror bland annat respondent 3 att:

> *" Men de som kommer att stå först på kö är de som har känsliga personuppgifter, då pratar vi vårdcentraler och apotek och såna företag står först på kö. Jag tror att det beror lite på hur hårt man slår till, alltså från myndighetssida".*

6. Analys

För att analysera den information som samlats in kommer informationen att ställas upp i olika tematiska tabeller som återfinns i bilaga B-E. Baserat på vad de olika respondenterna gett för svar har deras svar analyserats och jämförts mellan varandra baserat på egen tolkning och teoribakgrunden i arbetet.

De huvudsakliga teman som kan identifieras baserat på intervjuerna knyter nära an till de delfrågor som använts, kopplat till det första delmålet blir då huvudtemat ”rutiner vid säkerhetskopiering” och de olika delteman har identifierats som ”förändringar inför GDPR”, ”nuvarande backuprutin”, ”egen drift av backupsystem” och ”lagringslängd”. De olika delarna ställs därför upp i en matris med de olika delteman som identifierats och lämpliga urklipp av respondenterna svar, se bilaga B för matrisuppställningen för det första temat. Med uppställningen av datan kan man därefter konkretisera och analysera de olika respondenterna svar kring de olika delteman.

Tema 2 behandlar rätten att bli glömd och rutin för detta vid företaget, om de har en rutin, hur den ser ut och om den registrerade underättas vid borttagning av dennes information. Matrisuppställningen för detta team finns i bilaga C.

Tema 3 behandlar tekniska förändringar som skett vid företaget gällande säkerhetskopiering, detta kan vara t.ex. om företaget bytt vilket medium som nyttjas för säkerhetskopiorna som hur dessa skyddas och om detta är något som förändrats inför GDPR. Den tematiska matrisen finns i bilaga D.

Tema 4 behandlar hur verksamheterna och respondenterna ser på framtiden vad gäller säkerhetskopior och rätten att bli glömd, t.ex. hur andra företag har valt att anpassa sig och vad som kommer hända framgent. Den tematiska matrisen för detta finns i bilaga E.

6.1 Tema 1 – Rutiner vid säkerhetskopiering

Deltema 1 - Har ni gjort några förändringar inför GDPR?

Det som framträder tydligt i det första deltemat är bland annat att de flesta respondenternas verksamheter huvudsakligen verkar ha fokuserat på dokumentation och att få koll på sin data. Rent tekniskt verkar de ej som att några direkta rutinförändringar skett kring hur backuper tas, t.ex. granuarlitet och liknande. Respondent 2 lyfter till exempel fram att de har fått en ökad medvetandegrad om vilken information som faktiskt är deras ansvar och vilka krav som ställs på de. Till synes verkar det även som att respondenterna resonerar att de har har bra rutiner som det är och de därför ej anser att de behöver göra några förändringar gällande sina rutiner, detta framträder mest i respondent 3 och 5 svar men även i respondent 2 i intervjun. Detta stärks även av den osäkerhet som nämns i Brink, Elvland, & Hansson (2017) rapport där osäkerhet finns just kring hur man skall hantera säkerhetskopior.

Respondent 1 lyfter även upp en rutin som nämns utav Tankard (2016) att man aktivt styr åtkomst till informationen, detta genom att enbart viss personal har tillgång till informationen som de behöver. Detta kan anse stärka deras position gentemot åtkomststyrning då om enbart ett antal personer har åtkomst minskar alltså riskerna för säkerhetskopiorna.

Deltema 2 - Hur ser eran backuprutin ut?

Utav resultatet att döma har verksamheterna väldigt olika upplägg på ur ofta säkerhetskopior tas och vilken typ av säkerhetskopior det är som tas vid vilket tillfälle. På de kritiska systemen syns en högre frekvens av säkerhetskopiering än vid vanliga system. Respondent 2 och 3 är de som av att döma av analysen tar backuper oftast där detta genomförs med en täthet om var 15:e minut. Utöver detta är även frekvensen som säkerhetskopieringar tas på olika baserat på vilken typ av data som tas. Respondent 4 skiljer sig från mängden där de förlitar sig mer på ett system av replikering av sina databaser för att få redundans på systemen genom att de är spridda i olika regioner. Därefter tar de även en backup på en av de redundanta servrarna som enbart är en server som de går att läsa data ifrån men som tar emot replikering från de huvuddatabasen. Respondent 1 har även de en liknande lösning där de replikerar datan för att det skall gå snabbt att återställa och undvika driftstörningar genom att ha flera system. Att ha möjlighet att återställa informationen är något som omnämns specifikt i GDPR i artikel 32, del C i Europaparlamentens förordning (2016/679) och därför har verksamheterna en god förberedelse inför detta.

Något som kan vara tänkvärt kring informationen som det tas säkerhetskopior på är att man bör tänka på hur informationen är lagrad. Är den t.ex. lagrad i databaser bör dessa ha olika skydd. Ett exempel på detta är något som tas upp i Hintze & LaFevers (2017) rapport, där just psydonomisering utav informationen hjälper till att skydda informationen. Detta gäller även efter en återställning.

Deltema 3 - Sköter ni själva backuptagningen?

När intervjuerna och matrisen analyseras framträder tydligt att flera av respondenterna har de huvudsakliga systemen i externa serverhallar som de ej sköter det dagliga arbetet hos själva. Arbetet med att byta diskar och daglig drift sköts istället av en tjänsteleverantör som ser till att servrar är igång och att säkerhetskopior tas, detta gäller alltså respondent 2, 3 och 4. Respondent 5 verksamhet är den som äger egen serverhall och därför sköter all drift, övervakning och säkerhetskopiering själv och har full kontroll över vad som sker med den säkerhetskopierade datan, i intervjun framträder det att valet att ha en egen serverhall tydligt kan kopplas till externa krav som kommer ifrån deras kunder. Respondent 2,3 och 4 tar dock säkerhetskopior lokalt i sina arbetssystem också som de använder för att kunna återställa filer och versionshanteringssystem och liknande som sparas lokalt i samma hus som verksamheten bedrivs i. Respondent 2 är den som sticker ut mest då de har en hybridlösning där all data replikeras för att sedan säkerhetskopieras upp till molnet i backupform för möjlighet till återställning. Detta möjliggör att de ej behöver köpa egen lagring för att spara säkerhetskopior på.

Med den lösning som respondent 2,3, och 4 har valt innebär alltså att det finns ett delat ansvar om vad som sker med personuppgifterna som går igenom systemen, alltså bör personuppgiftsbiträdesavtal finnas på plats för att säkra (Datainspektionen, 2017i) legaliteten i att dela med sig utav informationen. Något annat som berörs här är även det tidigare arbetet om just molnleverantörers ansvar i Moe , Jaatun, Haugset, Niezen & Felici, (2013). Där nämns just att det ställs ett större ansvar för molnleverantören. Då måste man även säkerställa att t.ex. biträdesavtal finns på plats för att säkerställa legaliteten då informationen sparas på annan plats. Utöver detta är det viktigt att tänka på PbD för att säkerställa att att informationen som lagras hos leverantören är säker, även där.

Deltema 4 - Hur länge lagras backuperna?

Efter analys av den insamlade information framträder det att vissa av respondenterna antingen ej vet eller har en rutin för hur länge de sparar sina säkerhetskopior eller att de ej vill berätta detta p.g.a. företagshemligheter. Respondent 2,3 och 5 har däremot svar på hur länge deras säkerhetskopior kan sparas och det framträder tydligt att respondent 2 och 3 har en kort levnadstid på sina säkerhetskopior, detta då det oftast inte behövs återställas gammal information utan ” i och med att det inte är den gamla backup:en som behövs utan det är den senaste.”. De gamla backuperna används mest för att återställa enstaka filer som blivit raderade. Respondent 5 är dock den som lagrar säkerhetskopior längst där de maximalt lagrar säkerhetskopior på systemen 5 år, däremot genomförs en aktiv gallring utav uppgifter enligt det PUB-avtal som upprättas mellan kunden och respondentens verksamhet. PUB-avtal är något som aktivt krävs mellan ett företag och den personuppgiftsansvarige för hantering av uppgifterna enligt datainspektionen. Generellt finns inga styrningar kring just långtidslagring och säkerhetskopior men enligt Datainspektionen (2018h) är en maximal tid att spara information den tid som den faktiskt behövs, finns därefter inget behov skall informationen raderas. Därför om respondenternas verksamhet kan rättfärdiga lagringen genom laga stöd eller samtycke har de därför full rätt att lagra säkerhetskopior enligt de avtal som satts upp.

6.2 Tema 2 – Rätten att bli glömd

Deltema 1 - Finns en rutin på plats?

Överlag har samtliga respondenter en rutin på plats för att kunna ta bort personlig information i deras system, vilket är bra med tanke på det datum som allt skall vara klart på. Respondent 4 nämner däremot att de ej har någon klargjord rutin vilket de då kopplar till att de ej anse sig behöva detta med tanke på vilken information de sparar om de registrerade där bland annat mejladress innefattas i de uppgifterna. Enligt datainspektionen (2018g) räknas all information som kan ”direkt eller indirekt kan hänföras till en fysisk person som är i livet” till att vara en personuppgift, därigenom om mejladressen är sökbar eller om den är t.ex. ”pär.häzzvik@outlook.com” och man enkelt kan få fram vem den personen är i det verkliga livet bör detta alltså räknas som en personuppgift.

Jämförelsevis har alltså nästan samtliga företag valt att sätta upp en rutin eller åtminstone påbörjat en rutin, vissa manuellt och vissa ämnar automatisera processen för borttagning. Att ha en rutin på plats är en bra bit på vägen då det behöver finnas dokumenterat och klart (Datainspektionen, 2018i) till den 25:e maj, detta för att kunna påvisa hantering och radering utav personuppgifter vid en inspektion. Detta talar alltså till respondenternas verksamheters fördel att detta finns på plats.

Deltema 2 – Hur ser rutinen ut?

Bland respondenterna har respondent 2 och 3 ett liknande tänk kring borttagning och backuper, där de aktivt tar bort den registrerades information ur sina system som är aktiva, därefter låter de säkerhetskopiorna skriva över varandra till dess att den registrerades person har skrivits över, därefter betraktar de alltså borttagningen som slutförd. Detta är en problematik som tas upp Brink, Elvland & Hanssons (2017) arbete i intervjun med en av respondenterna som nämner just detta, att antingen tar man bort säkerhetskopiorna och den data som finns i nuvarande systemen, alternativ tar man bort personen och låter helt enkelt den registrerades information finns kvar i systemet. Något som t.ex. Politou, et al. (2017) anser vara fel där deras tolkning av GDPR är att även

information lagrad i backuper behövs tas bort, vilket de även nämner kan vara en svårighet (i många fall).

Respondent 1 däremot skiljer sig åt där de inte lagrar några backuper på den data som hanteras utav kunders system, utan de tar istället emot data från kunden som de sedan analyserar. Dock sker för en anonymsering av den information de tar emot. Detta sker för att undvika att behöva behandla uppgifter, avtal och liknande. Respondent 5 nämner däremot inget kring hur de tänkt hantera just backuper med avseende på rätten att bli glömd, mer än att backuper finns där av en anledning. Dock lyfter respondenten att de jobbar proaktivt genom att lösa problemen innan de uppstår och därigenom har de aldrig behövt genomföra en återställning utav deras information. Då respondent 4 inte har någon rutin för att bli bortglömd fanns därför ingen data att analysera, dock nämndes det att de mottagit fall där personer vill bli glömda och då har deras support-avdelning löst detta.

Deltema 3 – Informeras den registrerade vid borttagning?

Bland de intervjuade svarade här samtliga att det kommer ske en aktiv återkoppling kring borttagningen. Svaren varierar dock där t.ex. respondent 1 aktivt kommer meddela vilken information som blivit borttagen och vilken som de ej har blivit borttagen i och med andra lagkrav och liknande. Respondent 3 och 5 har här valt en enklare lösning där de enbart kommer rapportera att informationen som personuppgiftsansvarige har bett om att bli raderat har blivit borttagen.

6.3 Tema 3 – Tekniska förändringar av säkerhetskopieringar

Deltema 1 – På vilket medium lagras backuperna?

Bland respondenterna skiljer sig denna lagring åt kraftigt, där framkommer att respondenternas verksamheter lagrar på allt ifrån SSD:er till tape. Respondent 1 och 5 har lagringen på SSD:er för snabb åtkomst till informationen, vilket även kan vara till fördel om information skrivs över och tas bort p.g.a funktioner som t.ex. ”TRIM” kommandot. Respondent 2 har dock en intressant lösning där de inte själva lagrar några säkerhetskopior utan de istället lagrar sin information i en hybridlösning där informationen replikeras från den körande miljön till en server, informationen synkroniseras därefter med Microsofts backuplösning i molnet där de alltså är tjänsteleverantörer åt företaget. De har här ingen kontroll på vilken typ av medium som används utav Microsoft men de bär de fulla ansvaret för att informationen finns tillgänglig när den behövs. Detta kopplar an till Moe , et al. (2013) arbete kring molnleverantörers ansvarsområden gentemot sina kunder. De nämner där bland annat kommer i arbetet att det är molnleverantörens ansvar att säkra upp informationen som lagras i molnet och säkerställa dess tillgänglighet och skydd. Det är självklart även kunden till molnleverantörens ansvar att se till att ett tänk kring PbD finns med även här.

Respondent 3 har sin lagring både på disk och tape vilket bådar för långstidslagring men inte används för det, pga sin korta lagringstid kan dock en frågeställning växa kring om det verkligen behövs lagras på tape. Detta är dock självklart beroende på hur mycket information som passerar i systemen men i många fall borde en vanlig hårddisklösning vara fullt duglig. Viktigt att tänka på när det gäller hanteringen av lagringsmedium är att även detta inkluderas i konceptet PdB.

Deltema 2 - Har detta förändrats inför GDPR?

Det som är anmärkningsvärt här är att de flesta respondenterna inte har gjort några större förändringar inför GDPR gällande lagringen, men detta nog till viss del hänvisas till den ovisshet som finns och styrningar som saknar gällande just lagring och GDPR, något som flera av respondenterna nämner i intervjuerna. Respondent 1 skiljer sig dock åt här då de nämner att de aktivt jobbar med att förändra sina rutiner och hur de jobbar med saker därför kan det ej uteslutas att skiftet till SSD:er gjorts i samband med GDPR. Just lagringslösningar är något som alla kanske inte tänker på kring säkerhetskopior, men där framkommer vissa svårigheter, hur säkerställs att informationen verkligen är borttaget på t.ex. en säkerhetskopia som lagrats på band? I detta fall handlar det om tillit mellan verksamheten och leverantören. Kring lagring bör man konstant tänka kring PbD för att säkerställa att informationen som lagras tas om hand på rätt sätt.

Deltema 3 – Hur skyddar ni backuperna?

Samtliga respondenter förutom respondent 4 har i detta fall någon form av aktivt skydd utav sina backuper. Respondent 1 väljer här att ej avslöja något utan hänvisar till företagshemligheter vilket går att förstå, detta då säkerhetskopior i många fall är affärskritiska och därför vill ej alla prata om detta. Respondent 2 har här en ”klassisk” lösning på sina säkerhetskopieringar där de väljer att kryptera med nyckel som enbart de har tillgång till. Genom att säkra backuperna på detta sätt nämner även respondent 2 är fördel där de på ett sätt kan göra äldre backuper obrukbara, detta genom att byta nyckel på dessa och därigenom göra de oåterställningsbara. Detta skulle då ske i samband med att en registrerad vill bli bortglömd och därigenom göra äldre säkerhetskopior obrukbara. Att skydda säkerhetskopiorna genom kryptering är något som nämns utav (Datainspektionen, 2018j) som ett bra skydd av informationen, något som även nämnts i är psydonomisering utav den aktuella informationen (Ducato, 2016) genom att separera informationen och göra den svår att koppla ihop.

6.4 Tema 4 – Framtiden och andra företag

Deltema 1 - Andra företag och GDPR-anpassningar, backuper och rätt att bli glömd

Vad som framträder här är att det råder splittrad mening bland företagen men gemensamt här är att respondenterna anser att de tror andra företag har anpassat sig i den mån det går, med tanke på rådande lagstiftning och råd som getts. Respondenterna lyfter även här fram en del problem som vissa verksamheter kan ställas inför, respondent 1 tror att t.ex. ”en stor del av alla företag fortfarande inte har insett vikten av den här lagstiftningen” vilket tyder på en misstro mot andra verksamheter. Respondent 2 och 5 lyfter däremot upp andra verksamheter och tror att de flesta har gjort det som behövs efter sitt egna bästa kunnande vilket ändå tyder på en god tro inom branschen, något som respondent 2 nämner uttryckligen. Respondent 4 uttrycker även här en tro inom branschen att andra företag som hanterar större kvantiteter personuppgifter har anpassat sig mer inför GDPR.

När det kommer till säkerhetskopior och liknande tror respondent 3 att företag som kräver längre lagring av säkerhetskopior att de kommer få problem, detta kopplat till att det inte går att ta bort data ur säkerhetskopior utan antingen får man radera dessa vilket nämns av Brink, et al. (2017) eller låta de skriva över varandra. Dock blir det problematisk för de med långa lagringstider då datan ligger kvar, om än dock att den inte behandlas men den finns kvar.

Inför införandet av GDPR nämner även respondent 3 att de ser vissa problem i branschen, detta är t.ex. att få med sig hela organisationen i arbetet och att resuserna verkligen läggs på arbetet. Detta är något som bland annat lyfts utav (Tankard, 2016) som lyfter upp många av de delar som en organisation måste genomföra för att kunna vara redo. Det kräver alltså resurser från hela bolaget för att bli redo.

Deltema 2 - Vad kommer hända framgent?

Framgent råder en splittrad mening mellan respondenterna där de uttrycker viss oro över vad som kommer ske. Något som både respondent 4 och 5 däremot tycker är att beroende på hur mycket kontroll de registrerade vill ha över sin information kommer olika att hända.

Något som dock samtliga respondenterna delar är att de väntar med spänning vad som kommer ske efter den 25:e Maj när lagen träder i kraft, de råder även här lite delade meningar kring vad som kommer ske men vissa hyser tilltro till marknaden att arbetet kommer fortsätta medans t.ex. respondent 3 tror att flera företag kommer lägga ner arbetet i samband med att de anser arbetet slutfört.

7. Slutsats

Efter att intervjuer och transkribering skett har resultatet sammanställts och därefter har informationen analyserats. Genom analysen har även svar på delfrågor som ämnar besvara huvudfrågan i arbetet framkommit och de kommer nedan att behandlas.

På vilket sätt har verksamheterna förändrat sin rutin för säkerhetskopiering?

Generellt bland verksamheterna framträder tydligt att inga rutinmässiga förändringar har genomförts bland verksamheterna. Respondenterna har dock insett ett behov av att analysera vilken information de har och hur de hanterar denna och vem som har tillgång till den. Respondenterna har därför lagt mycket tid och arbete på att just lokalisera var informationen finns lagrad och vilka som har tillgång till informationen. Utöver detta har även en ökad ansvarskänsla framträtt bland respondenterna då de inser vilken information som är deras ansvar och att det ställs lagkrav på hur denna hanteras.

Något som även framträder här är att verksamheterna har en väldigt högfrekvent säkerhetskopiering på den information de hanterar, detta kommer tillåta snabb återställning som krävs enligt (Datainspektionen, 2018e) för att åter få tillgång till rätt information och personuppgifter vid potentiella haverier. Detta är dock inget som förändrats sedan tidigare men ändå hjälper verksamheterna att se till att ha funktionsdugliga system.

Utöver frekvensen och den rutinmässiga dokumentationen av information framträder det även att huvuddelen av verksamheterna är väl förberedda vad det gäller dokumentation och kontroll över säkerhetskopieringen.

Hur har verksamheterna utformat sin rutin för ifall någon vill bli bortglömd med avseende på säkerhetskopior?

Vad som framträder här är det råder delad uppfattning kring säkerhetskopior och lagrad information om de registrerade. Några av verksamheterna har här reflekterat kring just lagring av informationen i säkerhetskopiorna och resonerat att om de enbart lagrar säkerhetskopiorna en begränsad tid har de därför enkel möjlighet att ta bort information inom en kort tid då informationen kommer skrivas över när nya säkerhetskopior tas. Därför är informationen levande som högst 1-3 månader bakåt i tiden såvida det ej är aktuellt i produktionsmiljöer. Detta är något som diskuteras i dess legalitet i Brink, et al. (2017) samt Politou, et al. (2017) gällande vad och hur man skall gå tillväga för att faktiskt följa GDPR. Däremot är det generellt ingen av verksamheterna som aktivt raderar säkerhetskopior eller gör de oåterställningsbara efter att en borttagning skett.

Utöver detta nämner även huvuddelen av respondenterna att de även gallrar information efter en viss tid för att få bort information som ej behövs längre, därför försvinner även information ur produktionssystemen också utöver i säkerhetskopiorna. På det sättet sker en naturlig borttagning av information.

Gällande normal borttagning kommer verksamheterna att ta bort personen ur de system som de kan ta bort personerna ur, och fortfarande upprätthålla de lagar och regler som annars kan gälla. Exempel på lagar som kan förhindra borttagning är bokföringslagen och liknande där transaktioner skall sparas och även avtal och liknande.

Hur har verksamheterna rent tekniskt förändrat säkerhetskopieringen av information?

Bland respondenterna framgår att inga större förändringar skett vad gäller hur och på vad deras säkerhetskopior lagras, inte heller hur säkerhetskopiorna skyddas har ändrats inför GDPR. Däremot framkommer att just lagringsmedium är något som ständigt förändras i verksamheterna och därför är inte framtida förändringar att utesluta.

Vad gäller nuvarande lösningar har verksamheterna generellt sin lagring på vanliga hårddiskar men även kombinerat med molnlagring och säkerhetskopior på band som nyttjas för längre lagring. Utöver detta används även kryptering utav säkerhetskopiorna för att skydda de mot otillbörlig åtkomst utav de säkerhetskopior som sparas, något som t.ex. nämns explicit utav (Ducato, 2016; Tankard 2016) som ett rekommenderat sätt att skydda sin information på.
Något som även framkommer i intervjuerna är att flera av respondenterna väljer att inte driva sina egna servrar utan istället låter en tjänsteleverantör, en sk. kallad ”Hostingleverantör” som har serverhall med utrustning som de sedan hyr ut, driva deras fysiska servrar. Därefter styrs åtkomst till systemen och säkerhet kring detta i avtal mellan respondenternas verksamhet och respondenterna.

Hur ser verksamheterna på framtiden vad gäller säkerhetskopiering, rätten att bli glömd och GDPR?

Framtidsmässigt håller huvuddelen av respondenterna en god tro till övriga branschen att arbetet kommer fortsätta arbete med GDPR och att det inte kommer sluta anpassa sig. Utöver detta tror det även att det kommer komma framtida styrningar som kommer basera sig på prejudikat och liknande och där kommer branschen sedan att få anpassa sig därefter, t.ex. styrningar kring hur längre säkerhetskopior verkligen får lagras om inget behov finns.

För närvarande tror även respondenterna att andra företag bör ha kommit lika långt som de har gjort, dock lyfts det fram att de tror att det kan vara svårarbetat. Detta då GDPR är något som kräver hela organisationens hjälp och rätt resurser behöver tilldelas för att arbetet skall kunna fortskrida.

Utöver detta framkommer det även i intervjuerna att respondenterna beroende på medvetandegraden hos befolkningen kommer olika att ske gällande GDPR, är personer medvetna om GDPR tror respondenterna att flera kommer nyttja sig utav rätten att bli glömd och därmed kommer det leda till arbetet för organisationerna, något som nämns i tidigare stycken är t.ex. att ” Men de som kommer att stå först på kö är de som har känsliga personuppgifter, då pratar vi vårdcentraler och apotek och såna företag står först på kö.”. Därför kan alltså en korrelation dras att desto mer personuppgifter man sysslar med desto större sannolikhet att en verksamhet råkar ut för en inspektion från datainspektionen enligt respondenterna.

Forskningsfråga
”*Hur har mjukvaruutvecklingsföretag valt att anpassa sin backuptagning med tekniska och rutinmässiga förändringar inför GDPR samt vad har de för rutin gällande rätten att bli glömd?*

Företagen har i dagsläget ej genomfört några tekniska eller rutinmässiga förändringar vad gäller deras säkerhetskopior med avseende på GDPR och rätten att bli glömd. Fokus har varit att dokumentera nuvarande rutiner och få kontroll över all information verksamheten har samt hur den hanteras.

8. Diskussion

I följande del kommer arbetet som helhet att diskuteras. Inledningsvis kommer en diskussion föras kring metoden och resultatet och därefter samhällsnyttan samt etiska aspekter kring arbetet.

8.1 Metod

En styrka och svaghet i detta arbete är att 5 organisationer har intervjuats, samtliga utav företagen har varit belägna i eller nära Skövde och därmed har en geografisk avgränsning genomförts som därmed kan anses vara representativ för sektorn i detta område. Svagheten är här att just pga. Den geografiska avgränsningen kan detta resultat inte generaliseras över andra geografiska regioner då resultatet kanske inte är applicerbart där, beroende på vilka resurser och tillgångar som finns i ämnet där. Fördelen här är än dock att företag kan i detta arbete se vad mjukvaruutvecklingsföretag har genomfört inför GDPR och hur de tänkt kring hanteringen av säkerhetskopior och även rätten att bli glömd.

Under arbetets gång har allt granskats kritiskt, där framkom även att vissa utav frågorna som ställdes varit för snäva, där respondenterna nästan enbart kunna svara ”ja/nej”, där tanken egentligen varit att de skall bjuda in till diskussion och vara öppna i sin form. Detta kan därmed bidragit till att viss information inte framkommit i intervjuerna utan istället har detta förblivit dolt för den som genomför intervjun. Därmed drogs slutsatsen att intervjufrågorna kunde justerats något alternativt kunde uppföljningsfrågor ställts eller kunde respondenten blivit ombedd att utveckla kring frågeställningen. Dock har intervjuerna varit väldigt givande där de gett bättre insikt kring just frågeformulering och planering samt en ökad förmåga till att ställa lämpliga följdfrågor.

Utöver detta är det även lätt att göra en semistrukturerad intervju till en strukturerad genom att låsa sig vid manus. Detta märktes initialt i den första intervjun. Där måste den som intervjuar vara med och utveckla frågorna som ställs för att få ett uttömmande svar. Detta var en stor lärdom som tas med från skrivandet av rapporten.

Intervjuerna genomfördes i olika former, vissa genomfördes hos företaget, vissa genom Skype och vissa genom en bokad grupplokal. Därmed beroende på var intervjuerna genomförts kan nästan full anonymitet garanteras för respondenterna och en liten risk för identifiering finnes. Överlag genomfördes intervjuerna utan störningar, förutom tekniska problem till följd av driftstörningar och låg inspelningsnivå på ljudet. Generellt genomfördes intervjuerna även utan någon form av tidsbegränsning och respondenterna kändes avslappade och var även inte rädda för att lyfta de saker de såg som problematiska.

8.2 Resultat

Kopplat till andra arbeten som lyfter fram just problematiken syns det tydligt även här att resultaten kvarstår, t.ex. det som omnämns i Brink, Elvland & Hanssons (2017) rapport och interjuver att just säkerhetskopior är väldigt osäkert hur man skall ställa sig dessa. Däremot framkommer det även att tankarna kring problemet har även funnits hos respondenterna där en av de nämner just en potentiell hantering av säkerhetskopior genom att byta nyckel på säkerhetskopiorna och därmed göra de obrukbara. Utöver detta nämns även idéen att låta säkerhetskopiorna skriva över varandra vilket var en väntad idé. Detta då man då kan bibehålla affärskritisk information en tid tillbaka. Detta

säger dock direkt emot Politou, et al. (2017) arbete där de säger att rent legalt bör man faktiskt ta bort säkerhetskopiorna för att säkerställa att man följer GDPR.

Något som även här framträdde i intervjuerna var att dokumentationen av processer och var information finns var något som verksamheterna huvudsakligen fokuserat på, detta överrenstämmer med hyptosen som läggs fram i arbetet och är därmed glädjande och samtidigt bekymmersamt. Men då det ej finns några direkta styrningar och information som berättar om säkerhetskopior faktiskt är medtagna i rätten att bli glömd är det därför bara att invänta prejudikat och vidare styrningar från EU i frågan.

8.3 Samhällsnytta

Bidraget till omvärlden är framförallt att detta arbete ger en god insikt hur långt mjukvaruutvecklingsföretag har kommit i Skövde och runtom, samt hur de resonerat kring just GDPR och även rätten att bli glömd.

Allmänna rekommendationer till verksamheter har även här inkluderats vad gäller rutiner och även hur de bör resonera kring de olika aspekterna som denna rapport berört. Detta arbete kan både verka som en riktpunkt, hur långt företag i branschen har kommit inför GDPR och därmed även ge en inblick för andra mjukvaruutvecklingsföretag hur de ligger till och om de har tänkt på dessa aspekter som omnämns. Utöver detta bidrar även arbetet till att lyfta de några av delarna som respondenterna ser som problematiska och oklara med GDPR och därmed kan en röst höjas för att få klarhet i oklarheterna.

8.4 Etiska Aspekter

När arbetet publiceras finns alltid en risk för respondenterna att de eller deras verksamhet kan identifieras med hjälp av deras svar och därmed kan detta orsaka skada för respondenterna/verksamheterna. Därför har allting försökt anonymiseras i den mån det går, utan att dölja för mycket för att bibehålla en god validitet genom en viss spårbarhet.

Vissa av respondenterna har kännedom om varandra sedan tidigare, därmed kan inte full anonymitet i arbetet garanteras från respondenternas håll men de stycken och delar som är med i rapporten har ändå anonymiserats till den grad att det ej går att söka sig till företaget.

Det har tänkts kring anonymisering av ålder på företag och specifika roller för att undvika lättare identifiering av företagen, därför har åldern på företagen även maskerats och nämns ej i transkribering eller resultaten utan enbart respondentens roll tas upp, detta för att stärka validiteten i studien. Utöver detta har även respondenterna själva fått transkriberingarna för att kunna läsa igenom och avgöra om det finns felaktigheter eller rättelsebehov.

Ur en etisk synpunkt är resultatet bra. Detta beror på att nästan samtliga har dokumenterat sina rutiner och även satt upp rutiner gällande rätten att bli glömd. Den respondent som ej valt att genomföra något blir det problematiskt för, då även mejladresser är inkluderade i GPDR och därmed skall borttagning vara möjligt och det skall även finnas rutin för detta. Utöver detta är det både en etisk samt teknisk utmaning vad gäller GDPR och rätten att bli glömd då tekniska lösningar inte alltid finns att tillgå för att säkerställa att mänskliga faktorn utesluts vid borttagning av personer. Hur säkerställs att en person verkligen blivit borttagen? Verksamheterna bör ha tekniska kontroller och

liknande för att säkerställa borttagning. Detta är en viktig etisk aspekt att tänka på i arbetet med GDPR.

8.5 Framtida arbete

Då detta arbete framförallt har fokuserat på hur företagen har gjort inför införandet av GDPR kan ett intressant framtida arbete kontrollera vilka förändringar företagen genomfört längre fram i tiden. Detta när det kommit ett antal domar i domstol som därmed leder som prejudikat som därmed leder till ytterligare styrningar för företagen hur de skall anpassa sin verksamhet. Därför är det intressant att då kontrollera vidare vilka förändringar företagen har genomfört gällande sina säkerhetskopieringar och lagringstiden på dessa, baserat på vad som fastslagits i domar och prejudikat och då även kontrollera om några förändringar skett kopplat till om rätten att bli glömd även inkluderar säkerhetskopior.

Utöver detta kan det även vara intressant att i framtiden kontrollera olika backupsystem om det finns möjligheter i de att genomföra en återställning, men undvika att återställa vissa ”bortglömda” personer och hur detta skulle fungera.

Något som även kopplar an till hantering i backupsystem är PbD, där framtida system bör främja PbD genom dess användning och åtkomstkontroll. Där hade en kontroll kunnat göras hur utvecklingen ser ut kring PbD system som kan stötta automatisk identifiering av personuppgifter. Det hade även där varit intressant och se om det finns möjligheter att binda samman informationen från den automatiska identifieringen och backupsystem för att på detta sätt undvika återställning av borttagna personer, utan att namn eller liknande finns kvar sparat.

Referenser

Arkivnämnden. (2018). *Bevarande och Gallring | Regionarkivet*. Från Arkivnämnden: http://www.arkivnamnden.org/tillsyn-och-radgivning/bevarande-och-gallring [Hämtad 2018-05-30]

Beckett, P. (2017). GDPR compliance: your tech department's next big opportunity. *Computer Fraud & Security, vol 5*,ss 9-13.

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects, 2nd edt.* London: Springer-Verlag.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). Process for Data Protection Impact. *Privacy Technologies and Policy, 4th Annual privay forum* (ss. 21-37). Frankfurt/Main: Springer International Publishing, Switzerland 2016.

Bokföringsnämnden. (2017). *Arkivering*. Bokföringsnämnden: http://www.bfn.se/sv/fragor-och-svar/arkivering [Hämtad 2018-03-15]

Brink, J., Elvland, E., & Hansson, P. (2017). *Effekterna av GDPR.* Halmstad: Akademin för informationsteknologi - Högskolan i Halmstad.

Bryman, A. (2018). *Samhällsvetenskapliga metoder.* Stockholm: Libre AB.

BURTON, C., DE BOEL, L., KUNER, C., PATERAKI, A., CADIOT, S., & HOFFMAN, S. (2016). *The Final European Union General Data Protection Regulation.* THE BUREAU OF NATIONAL AFFAIRS, INC.

Data recovery. (2017). *What is the TRIM command on Solid State Drives?* Från Data recovery: https://datarecovery.com/rd/trim-command-solid-state-drives/ [Hämtad 2018-05-06

Datainspektionen. (2017a). *Förordningstexten*. Från Dataskyddsförordningen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#30 [Hämtad 2018-02-22]

Datainspektionen. (2017b). *Dataskyddsmyndighetens roll*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/dataskyddsmyndighetens-roll/ [Hämtad 2018-02-20]

Datainspektionen. (2017c). *De registrerades rättigheter*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ [Hämtad 2018-02-26]

Datainspektionen. (2017d). *Dataportabilitet*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/dataportabilitet/ [Hämtad 2018-02-22]

Datainspektionen. (2017e). *Rätt till radering*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-radering/ [Hämtad 2018-02-22]

Datainspektionen. (2017f). *Skadestånd*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/skadestand/ [Hämtad 2018-02-26]

Datainspektionen. (2017g). *Ansvarsskyldighet*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/principer-for-behandling-av-personuppgifter/ansvarsskyldighet/ [Hämtad 2018-04-19]

Datainspektionen. (2017h). *Dataskyddsombud*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsombud/ [Hämtad 2018-04-19]

Datainspektionen. (2017i). *Personuppgiftsbiträde*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsbitrade-och-bitradesavtal/ [Hämtad 2018-04-20]

Datainspektionen. (2018a). *Anmäla personuppgiftsincident*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/anmala-personuppgiftsincident/ [Hämtad 2018-02-25]

Datainspektionen. (2018b). *Klagomål*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/klagomal/ [Hämtad 2018-02-26]

Datainspektionen. (2018c). *Förordningstexten*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#32 [Hämtad 2018-02-26]

Datainspektionen. (2018d , Februari 23). *Administrativa sanktionsavgifter*.Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/dataskyddsmyndighetens-roll/administrativa-sanktionsavgifter/ [Hämtad 2018-02-27]

Datainspektionen. (2018e). *Förordningstexten*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/ [Hämtad 2018-03-05]

Datainspektionen. (2018f). *Molntjänster*. Från Datainspektionen: https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/ [Hämtad 2018-04-02]

Datainspektionen. (2018g). *Vad är en personuppgift?* Från Datainspektionen: https://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-en-personuppgift/ [Hämtad 2018-05-06]

Datainspektionen. (2018h). *Hur länge får uppgifterna i ett kundregister sparas?* Från Datainspektionen: https://www.datainspektionen.se/fragor-och-

svar/personuppgiftslagen/hur-lange-far-uppgifterna-i-ett-kundregister-sparas/ [Hämtad 2018-05-09]

Datainspektionen. (2018i). *Förberedelser för personuppgiftsansvariga*. Från Datainspektionen: https://www.datainspektionen.se/dataskyddsreformen/forberedelser/forberedelser-for-personuppgiftsansvariga/ [Hämtad 2018-05-09]

Datainspektionen. (2018j). *Allmäna råd - Säkerhet.* Retrieved from Datainspektionen: https://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf

De Hert, P., & Papakonstantinou, V. (2016, Mars 1). The New Police and Criminal Justice Data Protection Directive: A First Analysis. *New Journal of European Criminal Law, 7*(1), ss.7-19. doi:https://doi.org/10.1177/203228441600700102

Djurberg, J. A. (2018). *Kund fick ransomware – nu tvingas it-företag betala miljonskadestånd för bristande backup .* Från Computer Sweden: https://computersweden.idg.se/2.2683/1.696472/backup-skadestand [Hämtad 2018-04-15]

Ducato, R. (2016). Cloud computing for s-Health and the data protection - Getting ready for the General Data Protection Regulation. *016 IEEE International Smart Cities Conference (ISC2)* (ss. 1-4). Trento, Italy: IEEE. doi:10.1109/ISC2.2016.7580803

Eklund, G. (2012). *Interjvu som datainsamlingsmetod.* Åbo: Åbo akademi.

EU:s nya dataskyddsförordning GDPR - Fortnox. (2018, Februari 26). Från Fortnox: https://www.fortnox.se/blogg/eus-nya-dataskyddsforordning-gdpr/ [Hämtad 2018-03-20]

Flick, U. (2013). *An introduction to qualitative research.* London: Sage.

Hedin, A., & Martin, C. (2011). *En liten lathund om kvalitativ metod.* https://studentportalen.uu.se/uusp-filearea-tool/download.action?nodeId=459535&toolAttachmentId=108197 [Hämtad 2018-04-15]

Hintze, M., & LaFever, G. (2017). *Meeting Upcoming GDPR Requirements.* IAPP web conference service: IAPP web conference service.

Karlström, J. (2017). *Ramverk inför dataskyddsförordningen införande.* Skövde: Högskolan i Skövde.

Katayama, K., Chinda, Y., Shimizu, O., Mikami, T., Suzuki, M., & Noguchi, H. (2016, Juli). Long-Term Stability of Magnetic Tape for Data Storage. *IEEE TRANSACTIONS ON MAGNETICS VOL 52, NO. 7*, ss. 1.

Kvale, S. (1997). *Den kvalitativa forskningsintervjun.* Lund: Steinar Kvale och Studentlitteratur 1997.

Kvale, S., & Brinkmann, S. (2014). *Den Kvalitativa forskningsintervjun* (3:e ed.). Lund: Studentlitteratur AB.

Limoncelli, T., Hogan, C., & Chalup, S. (2007). *The practice of system and network administration, 2nd ed.* Upper Saddle River, NJ: Addison-Wesley.

Lindhe, J. (2018). *Detta har hänt: Facebook och Cambridge Analytica*. Från SVT: https://www.svt.se/nyheter/utrikes/detta-har-hant-facebook-och-cambridge-analytica [Hämtad 2018-03-09]

Moe , N. B., Jaatun, M. G., Haugset, B., Niezen, M., & Felici, M. (2013). *Cloud Accountability Project Workshop 1 Results.* Seventh framework Programme.

Multisoft. (2018). *GDPR - Vad är "privacy by design?"*. Från Multisoft: http://www.multisoft.se/gdpr/vad-ar-privacy-design/ [Hämtad 2018-05-30]

Papakonstantinou, V., & de Hert, P. (2016, December). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, ss. 179-194.

Politou, E., Alpeis, E., & Patsakis, C. (2017). *Forgetting personal data and revoking consent under the GDPR: Challeneges and Proposed Solutions.* Piraeus: University of Piraeus.

SOU 2017:39. (2017). *Ny dataskyddslag.* Stockholm: Elanders Sverige AB.

Sveriges Radio. (2018). *Få fälls för misstänkta brott mot PUL*. Från Sveriges Radio: http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5487830 [Hämtad 2018-03-25]

Tankard, C. (2016). What the GDPR means for businesses. *Network Security, 2016*(6), 5-8.

Wester-Lindgren, H. (2017). *EU-förordningar och direktiv*. Från Naturvårdsverket: https://www.naturvardsverket.se/Stod-i-miljoarbetet/Rattsinformation/Direktiv/ [Hämtad 2018-04-02]

Vetenskapsrådet. (2017). *God forskningssed.* Stockholm: Vetenskapsrådet.

Wohlin, C. (2012). *Experimentation in Software Engineering.* Berlin: Springer Berlin Heidelberg.

Bilaga A – Intervjuunderlag

Inledningsvis informeras de intervjuade om vad de innehar för rättigheter samt syftet med undersökning som genomförs.

Inledande frågor

- Vad har du för roll inom organisationen?
- Hur länge har du jobbat inom organisationen?
- På vilket sätt har du varit delaktig i införande av nya rutiner gällande GDPR?
    - Hur anser du att ligger till med avseende på den tid som finns kvar?
    - Har ni stött på några problem för att uppfylla GDPR?
    - Borde du blivit involverad?

Backuper

- Har du ingående kunskap i hur era backuper hanteras och rutiner för dessa?
    - Har du varit med och tagit fram dessa?
    - Varför har du ej varit delaktig i detta?
- Hur ser eran rutin ut i dagsläget gällande backuptagning?
    - Varför har ni valt att genomföra backuperna på det sättet?
    - Varför tar ni inte oftare eller mer sällan?
- Har denna förändrats något inför GDPR?
    - Vad har ni genomfört för förändringar gällande långtidslagring?
    - Vad har ni genomfört för förändringar gällande antal backuper som tas och när de tas?
    - Varför har ni ej genomfört någon förändring i backuptagningen?
- Har ni genomfört någon förändring med avseende på vilket media som nyttjas för backuper?
    - Vilken typ av media lagrar ni era backuper på idag istället?
    - Vilken typ av media lagrade ni tidigare på?
    - Vilken typ av media lagrar ni backuper på?
- Skyddar ni i dagsläget era backuper på något sätt?

    - Krypterar ni era backuper?
    - Vilken kryptografisk teknik används för att skydda säkerhetskopiorna?
    - Varför krypterar ni inte era backuper?
- Har ni någon form av arkivförvaring utav säkerhetskopieringar?
    - Hur ofta brukar ni få återställa från dessa?
    - Hur har ni tänkt hantera de med avseende på rätten att bli glömd?

Rätt att bli glömd

- Hur ser eran rutin ut ifall någon vill bli bortglömd?
    - Informerar ni den registrerade om när borttagningen är genomförd?

Framtiden

- Hur tror du att andra företag har valt att göra för att anpassa sig inför GDPR med avseende på backuper och rätten att bli glömd?
- Vad tror du kommer ske i Sverige framgent gällande GPDR och regler kring långtidslagring?

Avslutande fråga

- Är det något du skulle vilja tillägga?

Bilaga B – Rutiner vid säkerhetskopiering

	Har ni gjort några förändringar inför GDPR?	Hur ser eran backuprutin ut?	Sköter ni själva backuptagningen?	Hur länge lagras backuperna?
Respondent 1	”Ja, på backuper jobbar vi kontinuerlig med att förbättra och förändra oss och anpassa oss utifrån hur marknaden ser ut och hur lagkrav ser ut och hur vi kan jobba säkrare men vi jobbar ju i en förtroendebransch så att vi måste ha”	” Man kan inte riktigt gå in på det men vi gör ju såklart backup:er kontinuerligt, hela tiden och vi har fullständig redundans så att skulle något krascha så har vi allting någon annanstans”	-	-
Respondent 2	”Det som har förändrats är att vi har blivit mer medvetna om de krav som ställs och att det är vårt ansvar att hantera personuppgifter som kan finnas i backup-data”	”På filer tar vi som sagt var femtonde minut, på vissa kritiska databaser också var femtonde minut, andra med lite större mellanrum typ timmars men allting tas minst en gång om dagen som återställningspunkt.”	hybriduppsättning där vi har både on-prem backup:er med lite kortare intervaller och kortare livstid och sen lite längre lagring i molnet.	” R: Upp till 2-3 månader, men de flesta är kortare än så i och med att det inte är den gamla backup:en som behövs utan det är den senaste.”
Respondent 3	”Nej den har inte förändrats. Anledningen till det är att vi lagrar inte backuper längre tid.”	”Om vi tänker databasbackup tar vi en full backup per dag och sen tar vi varje timme transaktion, sen tar vi loggbackup:er, retention på de är, på transaktionbackup och loggbackup är 30 dagar.På fullbackup:en är det alltså fem cyklar. Alltså 5 veckocyklar”	”det är de som tar alla backup:er av vår produktion. Vi tar också backup:er, **hel och halvt???** på vår interna miljö, kontorsmiljö”	”5 veckocyklar”
Respondent 4	”Nej det har vi inte gjort någonting nu än. Så nej”	” Men iallafall är det en fullständig back up som tas varje timme. I ett initialt skede tas den backupen till en filserver i en annan region.”	”providers i båda fallen, men i det ena fallet är det på en filserver som vi har tillgång till själva medan den andra är en datastorage-lösning så att säga som vi kopierar	-

			till en annan provider som också har en cross region”	
Respondent 5	”Nej, det tror jag inte vi har gjort. Vi har ganska bra backup-system, liksom bra säkerhet och vi har bra tänk kring var vi har de här hallarna och så”	”Vårt huvudsystem backup:as varje halvtimme om jag förstår det rätt.”	”Vi har ganska bra backup-system, liksom bra säkerhet och vi har bra tänk kring vart vi har de här hallarna och så där så det är inget så vi har tänkt om.”	”maximalt 5 år”

Bilaga C – Rätten att bli glömd

	Finns en rutin på plats?	Hur ser rutinen ut?	Informeras den registrerade om borttagning?
Respondent 1	”Ja”	”Vår kunddata som vi har på våra kunders kunder skrotar vi så fort vi är klara med den, så man blir ju per automatik glömd.”	” om den skulle uppstå kommer vi såklart meddela när det är gjort och vilka saker de har rätt att bli glömda inom”
Respondent 2	”Ja”	” i och med att vi har en begränsad retention på våra backup:er så kommer den datan att försvinna.”	-
Respondent 3	” Alltså rutinen är inte helt klar än men den kommer att skötas via ett automatiskt system som heter Eloqua”	”Vi tar en användare och låter den försvinna ur nätverket då kommer den att försvinna ur våra backup:er senast efter fem veckor”	”Vi säger helt enkelt att vi har gjort det som du har bett om.”
Respondent 4	”Nej, inte från min sida iallafall då som sagt.”	-	-
Respondent 5	”vi är riggade för att plocka bort om de vill bli bortglömda”	”vi har möjlighet att hitta personen, plocka bort personen och de här bitarna”	”Ja, att vi har utfört arbetet gör vi ja.”

Bilaga D – Tekniska förändringar av säkerhetskopieringar

	På vilket medium lagras backuperna?	Har detta förändrats något inför GDPR?	Krypteras backuperna?
Respondent 1	” SSD, alltihop.”	” kontinuerligt med att hela tiden förändra och förbättra oss, så att vi byter ut vissa delar över tiden, självklart liksom, vi försöker hålla det modernt och bra.”	”Absolut, men det kan vi inte gå in på”
Respondent 2	”Vi har kört med molnbackup:er ganska länge nu och så det är disk och molnlagring och där bryr vi oss inte om hur, Microsoft då i det här fallet lagrar vår data.”	”Nej”	” det är en form av kryptering som bara går att avkryptera med nyckeln, det är ganska uppenbart men, att den kan inte lagras hos Microsoft var väldigt tydligt och det var det viktiga för oss
Respondent 3	”De lagras både på disk och på tape”	”Nej det är samma som vi kört innan”	” De är krypterade. Sen är de alla tagna till ett annat, separat datacenter som är endast för backup.”
Respondent 4	” Vi har inga egna tape-backups eller såna grejer”	-	” Det har inte implementerats än men det är någonting som varit i åtanke”
Respondent 5	”Jag tror att det är på SSD”	”nej”	”ja”

Bilaga E – Framtiden och andra företag

	Andra företag och GDPR-anpassningar, backuper och rätt att bli glömd	Vad kommer hända framgent?
Respondent 1	” Jag tror att en stor del av alla företag fortfarande inte har insett vikten av den här lagstiftningen”	” Jag tror även att många kommer fortsätta arbetet kring det för att göra det bra vad det lider och jag tror att en hel del företag inte är på banan till 25 maj.”
Respondent 2	” Man gör sitt bästa med hur man uppfattar lagen, så är det egentligen med alla lagar som påverkar verksamhet, men man gör det i good fate.”	” omöjligt men det är svårt att ställa sådana specifika krav som skall gälla alla i industri i och med att det finns så många olika behov och typ av verksamhets-business-modeller.”
Respondent 3	” För de som kräver långa backup:er, alltså det kommer bli högst problematiskt. Alltså om man inte ändrar rutinerna och minskar retention, eftersom det inte är något lätt verk att rensa ur en backup.”	”Men de som kommer att stå först på kö är de som har känsliga personuppgifter, då pratar vi vårdcentraler och apotek och såna företag står först på kö. Jag tror att det beror lite på hur hårt man slår till, alltså från myndighetssida.”
Respondent 4	” företag som hanterar just personuppgifter med namn och personnummer och såna grejer så har anpassat sig mycket mer inför såna här grejer då till exempel eftersom de personuppgifterna är närmare personen än vad kanske våra uppgifter är.”	”Men sen handlar det också om hur medvetna befolkningen över lag är om såna här grejer, om sina rättigheter.”
Respondent 5	”Jag tror att alla har gjort så mycket de kan, för alltså GDPR är rätt tydligt och det kommer ju så att. Jag upplever att vi och våra partners/konkurrenter är på tå där liksom”	”Jag tror väl så framöver kommer man rigga sig mycket mer för att kunderna själv, eller användare själv vill plocka sig in och ut och dölja sig och sånt, ja men kopplat till Facebook, man ser att folk är.”