LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

GDPR:s påverkan på IT-konsult-marknaden

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Theo Trotzig
Anas Sultan

Handledare: Benjamin Weaver

Rättande lärare: Magnus Wärja
Markus Lahtinen

GDPR:s påverkan på IT-konsultmarknaden

ENGELSK TITEL: The GDPR:s effects on IT-consultants

FÖRFATTARE: Theo Trotzig, Anas Sultan

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Odd Steen

FRAMLAGD: augusti, 2019

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 48

NYCKELORD: GDPR, integritet, privacy, privacy by design, IT-konsult

SAMMANFATTNING (MAX. 200 ORD):
Denna uppsatsens syfte är att studera hur införandet av GDPR påverkat IT-konsulter, även utmaningar som bör iakttas vid utveckling och implementering av IT-system. Utförandet av studien har framställts med hjälp av akademisk litteratur för att skapa en förståelse för privacy by design, samt för kraven GDPR sätter. Därefter samlades information genom kvalitativa intervjuer från verksamheter och IT-konsulter, och de hindren samt svårigheter de råkat ut för. Empirin har bestått av tre intervjuer som genomförts med IT-konsulter från diverse verksamheter, intervjuer har utförts med representanter från både privata och den offentliga sektorn. Vi har kategoriserat fem undersökningsområden utifrån intervjuerna; Digital integritet, informationsbehandling, informationssäkerhet, användarens rättigheter och ansvarsroller. Utifrån dessa kategorier analyserades empiri och litteratur för att sedan presenteras i resultatet.

Innehåll

Tabeller

1 Introduktion

1.1 Bakgrund

GDPR presenterades för första gången 2016 och trädde i kraft den 25 maj 2018, verksamheter har under de senaste 4 åren anpassat sig efter de nya kraven för behandling av data. Varje verksamhet måste vidta åtgärder i enlighet med GDPR:s föreskrifter, det finns diverse sätt att uppnå kraven som GDPR innehar. Föreskrifterna inom GDPR är ej teknikberoende, alltså är de teknikneutrala ((eu) GDPR 2016/679 27 april 2016). Då lagen är teknikneutral, krävs det inte något specifikt format för att hantera personuppgifter verksamheterna använder, kravet som GDPR har är att data bör vara i ett strukturerat, allmänt använt- och maskinläsbart format (Datainspektionen 20179b. Datainspektionen förespråkar även interoperabilitet, verksamheter som är inom en gemensam bransch eller sektor bör gemensamt samarbeta för att implementera branschstandarder för sektorn i fråga (Datainspektionen 2019b).

Det kan uppkomma begäran av dataportabilitet för den data verksamheten tillhandahållits av användarna (Datainspektionen 2019b), vilken data som ska anses som det har tillhandahållits av användaren, avgörs av verksamheten, samt förväntas verksamheten uppfylla användarnas förväntningar av vilka personuppgifter verksamheten behandlar. Vid dataportabilitet måste personuppgiften extraheras samt identifieras, detta leder till att vissa utmaningar och problem kan uppkomma för verksamheten, dessa svårigheter kan till exempel uppstå på grund av att organisationen använder sig utav flertal system.

När presenterades GDPR var inte det första gången som det framförts förslag för att förbättra informationssäkerhet och att öka integritet när det kommer till individers personinformation. I juni 2010 framfördes ett förslag för en nationell strategi för att skapa ett ”identity ecosystem”, en onlinemiljö där individers och organisationers digitala identiteter bevisas och skapar därför tillit. Målet med detta ekosystem är att öka säkerhet, effektivitet och integritet (W House 2011). Detta kräver att individer ger ut sin personinformation till en tredje part så att den kan autentisera alla involverade parter. Detta anser Crossler och Posey kräver att individer riskerar sin informations integritet för att öka säkerheten. Detta med grunden att dessa centraliserade dataförvar blir mål för stater och kriminella för att spåra individer och organisationers webtrafik och på så sätt invadera deras integritet (Crossler, Posey 2017). Under 90-talet började Cavoukian fokusera på hur teknologi kunde förbättra informationsintegritet då detta grundades i juridiska krav (Cavoukian 2010). Detta vidareutvecklade Cavoukian sedan till ”Privacy by design” och delade upp detta i sju grundprinciper (Cavoukian 2009). Privacy by design är något som omnämns ofta i samband med GDPR och anses vara ett sätt att uppfylla GDPR:s krav på (Datainspektionen 2019d).

1.2 Problemområde

Dataportabilitet har på sätt och vis lett organisationerna till att anpassa sig till lagstiftningen genom att utföra organisatoriska samt tekniska korrigeringar. Organisationer bör utforma en uppfattning om deras användare, var de får deras uppgifter ifrån och även var i systemet användarnas data lagras. När en verksamhet strider mot regler från förordningen, kan det leda till att verksamheten bli åtalad till en sanktionsavgift vilket kan vara upp till 4% av omsättningen verksamheten haft årligen (Datainspektionen, 2019b). GDPR uppmuntrar till att branscherna ska samarbeta, även konkurrenterna inom samma sektor uppmuntras till att gemensamt standardisera åtgärder som bör tas för att uppnå målen och förväntningarna från användarna och GDPR.

Under 2018 så rapporterades 2262 personuppgiftsincidenter till Datainspektionen varav 61 procent berodde på mänskliga faktorer, 14 procent på antagonistiska angrepp och 8 procent på bristande organisatoriska rutiner eller processer (Datainspektionen 2019a). Detta betyder på att det var många organisationer som inte helt uppfyllde kraven även efter GDPR trätt i kraft. Under våren 2019 har Datainspektionen inlett tillsyn vid tre separata tillfällen på 1177 vårdguiden och inlett granskning av 8 större sjukhus och sjukvårdsorganisationer och även en mot Klarna (Datainspektionen 2019f, g, h). Efter en incident så notifierade British Airways ICO, den brittiska dataskyddsmyndigheten, i september 2018. Efter en utredning har ICO gjort uttalande om att de har till intention att bötfälla British Airways 183,39 miljoner pund (ICO 2019a). ICO har även gått ut med att de har intention att bötfälla Mariott International över 99 miljoner pund för en incident som startade år 2014 i ett bolag som de köpte 2016 och slutligen notifierades till ICO i november 2018. Slutsatsen från ICO:s undersökning var att Mariott inte gjorde tillräckligt för att säkra sina system (ICO 2019b). Dessa åtgärder pekar mot att det fortfarande idag finns stora brister när det kommer till hur organisationer hanterar personuppgifter och hur de inte uppfyller GDPR:s krav.

1.3 Frågeställning

Då GDPR är fortfarande en ny lagstiftning så finns det få studier kring dess konkreta konsekvenser. De studier som utförts fokuserar ofta på GDPR:s påverkan på systemutvecklingsprocessen. Bristen av litteratur med fokus på IT-konsulter ledde resulterade i vår forskningsfråga:

Hur har IT-konsulter påverkats av GDPR?

1.4 Syfte

Syftet med denna studie är att identifiera hur konsultbolagen går tillväga för att uppfylla GDPR:s databehandlingskrav. Med hjälp av vår empiri från kvalitativa intervjuer vill vi identifiera de största svårigheterna för IT-konsulter att upprätthålla lagring och skydd av information enligt GDPR:s krav. Vi även syftar till att addera kunskap till forskningsområdet och se hur det har förändrats sedan GDPR trädde i kraft genom att ge en inblick i det praktiska påverkningarna GDPR har haft på IT-konsulter.

1.5 Avgränsningar

Vi har valt att fokusera på hantering och skyddsaspekterna av GDPR och kommer därför inte att beröra resterande aspekter. Vi har inriktat oss på IT-konsulter och deras lösningar och hur de påverkas av GDPR och avgränsar oss även från interna IT-projekt där konsulter inte varit inblandade.

2 Litteraturgenomgång

Litteraturgenomgången inleds med en kort beskrivning av de delar av GDPR som är relevanta för forskningsfrågan. Det följs av en granskning av informationssäkerhetsteorier och avslutas med en granskning av Privacy by design.

2.1 GDPR

2.1.1 Behandling av personuppgifter

I artikel 5 i GDPR definieras principer för behandling av personuppgifter och redogörs för nedan.

1.
    a) Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade ((EU) 2016/679, artikel 5.1a).
    b) Personuppgifter ska samlas in för särskilda, berättigade och uttryckta ändamål ((EU) 2016/679, artikel 5.1b).
    c) Personuppgifterna ska vara relevanta till de uttryckta ändamålen ((EU) 2016/679, artikel 5.1c).
    d) Personuppgifterna ska vara korrekta och uppdaterade. Det ska säkerställas att felaktiga uppgifter raderas eller rättas ((EU) 2016/679, artikel 5.1d).
    e) Personuppgifterna ska inte förvaras i en form som gör dem identifierbara av den registrerade under en längre period än ändamålet kräver ((EU) 2016/679, artikel 5.1e).
    f) Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet med användning av tekniska eller organisatoriska åtgärder ((EU) 2016/679, artikel 5.1f).
2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 följs ((EU) 2016/679, artikel 5.2).

2.1.2 Privacy by design och privacy by default

I artikel 25 i GDPR nämns inbyggt dataskydd och dataskydd som standard, också kallat privacy by design och privacy by default. Dessa anses vara sätt att uppfylla GDPR:s krav på hur information behandlas, anonymiseras och lagras ((EU) 2016/679, artikel 25).

Inbyggt dataskydd innebär att organisationen tar hänsyn till integritetsskyddsreglerna när man utformar IT-system och rutiner. Dataskydd som standard innebär att den som behandlar personinformation måste se till att information inte behandlas i onödan, så som att de förvalda inställningarna är satta så att information inte samlas in eller visas i onödan (Datainspektionen 2019d).

2.1.3 Rätten till att ta del, uppdatera och radera sin personinformation

Användare har rätt att kontakta en organisation och begära att få veta vilka personuppgifter och i vilket syfte organisationen behandlar dem genom ett registerutdrag. Detta utdrag ska innehålla information om vilka uppgifter som behandlas, hur de behandlas, var de kommer ifrån, behandlingens syfte och till vilka uppgifterna har lämnats ut (Datainspektionen 2019c).

Användare har även rätt att kontakta organisationer som behandlar deras uppgifter och be om att få uppdatera felaktig personinformation. Användaren har även rätt att komplettera personuppgifter som saknas och är relevanta för informationsbehandlingen (Datainspektionen 2019c).

Alla användare har även rätt att kontakta företag och be att deras uppgifter raderas. Detta innebär att organisationen måste informera dem som de har lämnat ut användarens uppgifter till. Detta med syfte att kopior eller länkar till uppgifterna också raderas (Datainspektionen 2019c).

2.1.4 Personuppgiftsansvariga och personuppgiftsbiträden

Den som behandlar personuppgifter kan kategoriseras som antingen personuppgiftsansvarig eller som ett personuppgiftsbiträde. Den personuppgiftsansvarige är den som etablerar i vilket syfte uppgifterna behandlas och hur detta utförs medan personuppgiftsbiträdet är den som behandlar personuppgifterna i den personuppgiftsansvariges räkning. Dessa kan vara allting ifrån en fysisk eller juridisk person till en organisation eller offentlig myndighet. De som behandlar personuppgifter har ansvar att se till att det görs enligt dataskyddsförordningens, den svenska implementeringen av GDPR, krav (datainspektionen 2019e).

Om två eller flera etablerar en viss behandling tillsammans blir de gemensamt personuppgiftsansvariga och måste de bestämma vem av dem som är ansvarig för att uppfylla kraven från dataskyddsförordningen. Den som är ansvarig kan sedan överlåta behandlingen personuppgifter men det är inte möjligt att överlåta ansvaret. Det är även upp till den ansvarige att se till att behandlingen uppfyller dataskyddsförordningens bestämmelser och att genomföra tekniska och organisatoriska åtgärder för att säkerställa detta. Detta kan göras genom att ha en policy med strategier som säkerställer detta eller genom diverse certifieringar (Datainspektionen 2019e).

Det finns alltid ett personuppgiftsbiträde utanför den ansvariges organisation. Det är upp till det anställda biträdet att garantera att behandlingen uppfyller dataskyddsförordningen och att den registrerades rättigheter är skyddade. Biträdet och dess personal får endast behandla uppgifter per instruktion från den ansvarige och får inte anlita ett annat biträde utan ett skriftligt tillstånd från den personuppgiftsansvarige. Några av de skyldigheter som har gällt för den personuppgiftsansvarige gäller även nu för biträdet, som att föra register för behandlingar, att säkerställa en säkerhetsnivå och ibland att utse ett dataskyddsombud. Både den ansvarige och biträdet kan bli föremål för tillsyn eller sanktionsavgifter om dataskyddsförordningen inte följs (Datainspektionen 2019e).

2.2 Informationssäkerhet

2.2.1 CIA

Enligt Wylder (2003) kan informationssäkerhet bli sammanfattad till tre aspekter, dessa tre aspekter lyfts fram i CIA-triaden, vilket är en teori som blivit erkänd och som används inom informationssäkerhet. CIA-triaden innehar tre beståndsdelar, dessa är: Integrity, confidentiality och availability. Beståndsdelarna inom CIA-triaden anses som basen när det gäller säkerhetsprogram då de har en hopkoppling med konceptet av informationssäkerhet.

Integrity

Integritetskomponenten av CIA-triaden, har fokus på att "upprätthålla korrekt och fullständig information som inte har ändrats av obehöriga användare eller processer" (Wylder, 2003). Det mest vitala med integritetskomponenten är att data ej får ändras av användare som inte är behöriga under tiden data överförs, och om det skulle ske att någon obehörig gör ändringar, så borde det finnas möjlighet för att återställa och få tillbaka den ursprungliga datan via en "backup".

Den känsliga datan bör skyddas via att det finns åtkomstkontroll samt rättigheter. Användarna som har förfogande för den känsliga datan får inte använda den på fel sätt. Det kan leda till skadegörelse samt påverka integriteten. En säkerhetsåtgärd för att säkra integriteten kan vara brandväggar, intrångsdetektering som vid en del tillfällen kan upptäcka förändringar i data via EMP (elektromagnetiska pulser) och kommunikationssäkerhet (Agarwal & Agarwal 2011).

Availability

Fokusen i aspekten availability ligger på att användare ska ha pålitlig samt aktuell möjlighet att utnyttja informationen (Wylder, 2003). Tre delar måste funka samt vara ihopkopplade för att användarna ska ha tillgång till informationen, delarna är: Säkerhetskontroller som försvarar information, system som lagrar data och tillgänglighet för kommunikationskanaler (Agarwal & Agarwal 2011). Företag borde hela tiden underhålla sin säkerhet för nätverk, hårdvara som har uppdateringar samt kunna utföra reparationer vid tillfällen då det behövs.

Confidentiality

(Wylder, 2003) förklarar att aspekten Confidentiality förhindrar data från att bli öppen för obehöriga. Innebörden av confidentiality (konfidentialitet) är likt sekretess, informationen behöver en design som är adekvat som kan stoppa känslig data från att vara öppen och tillgänglig till de som inte har behörighet, samt tillåter behöriga komma åt data. Data som behandlas bör klassas utifrån graden samt sorten av skada som riskeras att hända, detta kommer sen avgöra vilken nivå av säkerhet samt konfidentialitet som behövs.

Agarwal & Agarwal (2011) anser att organisationer som vill säkra deras konfidentialitet av information bör ha nätverksautentiseringstjänst, nätverkssäkerhetsprotokoll, samt krypteringstjänster. Företag borde erbjuda alla deras anställda en säkerhetskurs som går igenom alla de vitala delarna gällande informationssäkerhet, kursen ska även informera de anställda om konsekvenserna som kan drabba de anställda och företaget om någon obehörig kommer åt känslig data.

2.2.2 RITE

RITE ligger nära CIA-triaden och är en annan modell inom informationssäkerheten, det kan även anses som en utvecklande modell av CIA-triaden. Dhillon & Backhouse (2000) framställde informationssäkerhets modellen RITE med tanken att modellen skulle fungera som ett tillägg till CIA-triaden inom organisationer. Meningen var att RITE skulle öka säkerheten för verksamheter. Dhillon och Backhouse (2000) menar att CIA-triaden fokuserar på vetenskap och industrier via grundläggande handlingsprogram och anser att CIA-triaden brister inom strategiskt förhållande. Genom att implementera RITE, en utveckling som innehåller de strategiska aspekterna som saknas i CIA-triaden, menar Dhillon & Backhouse (2000) att de brister som finns i CIA-triaden kompletteras och ökar verksamhetens informationssäkerhet. RITE består av fyra delar som redogörs nedan.

Responsibility

Responsibility riktar in sig på att förstå rollen man har i verksamheten, samt vilket ansvar som uppstår inom den rollen man har (Dhillon & Backhouse 2000). Denna komponent som fokuserar på ansvar, lägger viktig för rollbäraren att ha vara medveten om hur stort dess ansvar är. När det tillkommer ett fel i verksamheten är de viktigt att de som är ansvariga ska ha koll på det och även stå till svars.

Integrity

Dhillon & Backhouse (2000) förklarar integrity aspekten som den anställdas integritet inom en organisation. Verksamheter bär på känslig data, så det är väldigt kritiskt för verksamheterna att ha reda på vilka det är som har tillgång till den känsliga data, samt så ska verksamheterna ha koll på riskerna för de anställda att bryta deras integritet och missanvända den känsliga informationen verksamheten har.

Trust

Trust-aspekten lägger fokus på verksamhetens förtroende för deras anställda. Finns det ett starkt förtroende kan det användas som en typ av säkerhet.

Ethicality

Sistnämnda aspekten i RITE-teorin handlar om etik och fokuserar på besluttagandet av de anställda och om dessa beslut är enligt etiska metoder (Dhillon & Backhouse. 2000). Besluten är normer och inte är regler i verksamheten, dessa besluttaganden anses som icke-formella normer.

2.2.3 Diligence Model

The diligence approach framför hur modellen kan lösa problem som hade uppstått om man bara utgått ifrån CIA-triaden (Al-Hamdani 2009). Al-Hamdani menar att CIA-triaden i sig inte är tillräcklig i alla fall när det gäller säkerheten, Al Hamadi menar att man bör uttöka CIA-triaden och bygga vidare på teorin. Ett exempel som Al Hamadi tar upp är, när en bärbar dator blir stulen, där data är privat och känslig, i detta fall finns integriteten av informationen kvar, men användaren har ej tillgång till datorn då den är stulen, i detta ecempel håller inte CIA-triaden.

Det Al-Hamdani (2009) gör är att implementera tre nya aspekter till CIA-triaden, aspekterna är:

- Utility – användbar Information för ett visst syfte
- Possession/Control – hålla, kontrollera och kunna använda
- Authenticity – Validitet, överensstämmelse och genuinitet av informationen

Aspekterna som är tillagda till triaden har syftet att underlätta vid situationer som har en risk att uppkomma när man jobbar med informationssäkerhet.

2.3 Privacy By design

Europeiska unionen definierar privacy by design som att implementera tekniska och organisatoriska lösningar i de tidigaste designstadierna av databehandlingsprocesser så att information skyddas från början (EU, 2018). Målet med privacy by design är att det är integrerat i designen av systemet så att det inte behövs läggas på i efterhand som en modul. Privacy by design lägger vikt i att säkerhet måste integreras tidigt men definierar inte vad som konkret behövs göras (Gürses, Troncoso & Diaz, 2011). Gürses et. al. uttrycker att det finns risker med att privacy by design utformas till en kravlista som bör anpassas till alla typer system. Detta kan leda till falska uppfattningar om integritet och förtroende och att teknikneutrala kravlistor löper stor risk att användas för att samla in all data av intresse (Gürses et. al. 2011).

2.3.1 Privacy by designs sju grundprinciper

Cavoukian (2009) anser att privacy by design måste, på samma sätt som andra aspekter av digital design, ses utifrån ett holistiskt, innovativt och integrerande perspektiv. Cavoukian (2009) Delar upp privacy by design i sju grundprinciper för att tydliggöra och skapa ett referensramverk.

1. Proactive not reactive; Preventative not remedial

Privacy by design karaktäriseras av att vara proaktivt och inte reaktivt. Det förväntar och förebygger integritetsintrång innan de händer. Privacy by design väntar inte på att risker ska materialiseras och har inga lösningar för att åtgärda intrång när de har hänt utan siktar på att förebygga dem från att inträffa. Detta kräver tydligt engagemang från ledning att sätta hög standard på integritet som genomsyrar hela organisationen och dess kultur. Det innebär även att det behövs etablerade metoder för att identifiera bristfällig integritetsdesign och att systematiskt förebygga dessa (Cavoukian 2009).

2. Privacy as the default

Privacy by design sätter som mål att leverera den högsta graden och integritet genom att säkerställa att data automatiskt skyddas i alla IT-system och organisationsprocesser. Om en individ inte utför något så är deras integritet fortfarande skyddad. Det finn inga krav på att individer ska ta några steg för att skydda sin information, det ska vara inbyggt i systemet. Detta kan ses som privacy as default och grundas i fyra delar. Purpose Specification, att anledningen till att personinformation samlas, lagras och används ska kommuniceras med individen samtidigt eller innan den samlas in. Detta ska vara tydligt, begränsat och relevant. Collection Limitation innebär att insamling av personinformation ska vara rättvis, laglydig och

begränsad till sitt syfte. Data Minimization, att insamlingen av personidentifierbar information bör hållas till ett minimum. Designen av program, information och kommunikationsteknologi borde börja med anonymiserade transaktioner som standard och minimera indentifierbarhet, observationsmöjlighet och koppling i största möjlighet. Use, Retention and Disclosure Limitation, att användning, lagring och avslöjande av personinformation ska begränsas till de relevanta syftena som är identifierade till individen och som hen har gett samtycke till, med avgränsning till lag. Personinformation ska bara lagras så länge den behövs för att uppfylla det uttalade syftet och sedan säkert raderas (Cavoukian 2009).

Där behovet av personinformation är otydligt ska det antas att integritet och försiktighetsprincipen ska användas. Standarden ska alltid var den mest integritetsskyddande (Cavoukian 2009).

3. Privacy embedded into design

Privacy by design är inbyggt i designen och arkitekturen av IT-system och organisationsprocesser, det läggs inte till i efterhand. Resultatet blir att integritet blir en essentiell komponent i kärnfunktionaliteten som levereras. Integritet är integrerat i systemet utan att påverka funktionaliteten. Integritet måste vävas in i designen på ett systematiskt sätt som stöds av accepterade standarder och ramverk. Där det finns möjlighet bör detaljerade riskbedömningar utföras, dokumenteras och publiceras, dessa ska även innehålla vad som utförts för att minska dessa risker (Cavoukian 2009).

4. Full functionality – positive-sum, not zero-sum

Privacy by design strävar mot att uppfylla alla legitima mål på ett sätt där alla involverade parter tjänar på det. Privacy by design undviker anspråk som privacy by design mot säkerhet genom att demonstrera att det är möjligt och mer eftertraktat att uppfylla båda. Privacy by design innebär inte bara att visa engagemang, det innebär att uppfylla alla legitima mål, inte bara integritetsrelaterade. När integritet vävs in i ett system eller en process så bör det göras utan att påverka funktionalitet och att alla systemkrav är optimerade (Cavoukian 2009).

5. End-to-end security – lifecycle protection

Efter att privacy by design har vävts in i systemet innan den första datan samlats in så måste det fortsätta genom hela livscykeln av insamlade data. Det är essentiellt med hög säkerhet för att bevara integriteten, både på hur den samlas in och hur den raderas. Integritet måste skyddas kontinuerligt genom hela livscykeln och det får inte finnas några luckor i varken säkerhet eller ansvarighet (Cavoukian 2009).

6. Visibility and transparency

Privacy by design strävar mot att säkerställa för alla intressenter att systemet eller processen fungerar som den ska enligt överenskommelser. Detta görs genom att systemet eller processen är synlig och transparent för både användare och leverantörer. Med tillsyn i åtanke kan detta fokuseras på tre aspekter, Accountability, Openness och Compliance. Accountability innebär att ansvaret för integritetsrelaterade policys och processer dokumenteras och tilldelas till en specifik individ. Openness syftar till att transparens är nyckeln till ansvarighet. Information om policys och processer som är relaterade till hanteringen av personinformation ska vara tillgänglig till individen. Compliance innebär att processerna för klagomål ska vara etablerade och ska kommuniceras till individen, inkluderat hur man överklagar. Det innebär även att det

nödvändiga stegen för att övervaka, evaluera och säkerställa att integritetspolicys uppfylls (Cavoukian 2009).

7. Respect for user privacy

Privacy by design sätter krav på att arkitekter och användare fokuserar på att individers intresse skyddas. Det innebär att det måste finnas integritetsstandarder, notifiera i tid och framföra användarvänliga alternativ. De bästa resultaten kommer oftast från medvetna designbeslut som kretsar kring individers behov då dessa har det största intresset av att bibehålla kontroll över deras personinformation. Att ge individer en roll i hanteringen av deras personinformation kan vara det mest effektiva sättet att skydda mot missbruk av integritet och personinformation. Detta stödjs av fyra aspekter, Consent, Accuracy, Access och Compliance. Consent innebär att individers samtycke krävs för att samla, använda eller avslöja personinformation bortsett från vissa juridiska situationer. Samtycke kan tas tillbaka när som helst utan angiven anledning. Accuracy syftar till att personinformation ska vara så exakt, fullständig och aktuell som möjligt för att uppfylla sitt syfte. Access innebär att individer ska ha tillgång till sin personinformation och informeras om dess användning och syfte. Individer ska även kunna rätta till fel i sin personinformation. Compliance innebär att organisationer ska ha system för att ta emot klagomål (Cavoukian 2009).

2.3.2 Privacy design strategies

Hoepman (2014) anser, likt Cavoukian, att privacy by design måste vara närvarande från första tanke till sista steget i utvecklingsprocessen. Då lagverk som GDPR nu sätter krav på att privacy by design ska vara integrerat så har Hoepman (2014) tagit fram åtta privacy designstrategier tifrån designmönster och existerande lagverk som hanterar dataskydd med mål att hjälpa IT-arkitekter att implementera privacy by design så tidigt som möjligt i utvecklingsfasen. Stora delar av dessa strategier finns även grundande i artikel 5 samt 25 i GDPR ((EU) 2016/679).

1. Minimise

Den mest grundläggande strategin är att minimera lagring av personinformation så mycket som möjligt. Genom att säkra att så ingen data lagras i onödan minskas konsekvenserna av dataintrång. Genom att använda denna strategi så uppstår inga frågor om data lagras utan syfte eller om det finns mindre påträngande alternativ till att uppnå samma syfte (Hoepman 2014). Detta är något som Gürses et. al. (2011) också lägger stor vikt i att minimera lagring av personinformation men även att limitera insamling av den.

2. Hide

Genom att gömma personinformation så blir den svårare att utnyttja. Denna strategi specificerar inte vem informationen ska döljas för, detta är beroende på kontexten där den appliceras. I vissa fall så bör informationen döljas från alla, i andra fall så som när personinformation samlas in bör den döljas från tredje parter. Denna strategi är essentiell och förbises ofta vilket har resulterat i att identifierare i systemen orsakat integritetsproblem. Målet med denna strategi är

att säkra att händelser inte kan kopplas samman och att sänka observerbarheten (Hoepman 2014).

3. Separate

Denna strategi menar att personinformation ska bearbetas distribuerat och om möjligt i separat från varandra. Genom att separera bearbetningen och lagringen av flera personuppgifter som tillhör samma individ så hindrar man möjligheten att hela profileringar kan samlas. Det är även ett bra sätt att limitera bearbetning och lagring av data till dess syfte. Separationsstrategin kräver distribuerad bearbetning och inte centraliserad, framförallt bör data från olika källor lagras i olika databaser som inte är kopplade till varandra. Information bör bearbetas lokalt och om möjligt också lagras lokalt. I dagens IT-klimat där fokus ligger på centraliserade webbaserade lösningar så bortprioriteras denna strategi ofta, även om integritet skyddas avsevärt bättre genom peer-to-peer-nätverk. Decentraliserade lösningar är i grunden säkrare än centraliserade (Hoepman 2014).

4. Aggregate

Denna strategi grundas i att personinformation bör sammanfogas till så stora samlingar som möjligt med så lite detalj som möjligt i den mån om att den fortfarande är användbar till sitt syfte. Genom att sammanfoga information i attributet eller grupper av individer så begränsas den sammanfogade informationens detaljrikhet och blir mindre känslig. När personinformationen blir mindre detaljrik och sammanfogas i tillräckligt stor grupp så kan informationen nästan inte längre kopplas till en specifik individ och skyddar dess integritet (Hoepman 2014).

5. Inform

Den femte strategin grundas i transparens och att individer vars data bearbetas ska informeras om detta. När en individ använder ett system så bör de informeras om vilken information som bearbetas, även i vilket syfte och utsträckning. Detta innefattar även att informera om hur informationen skyddas och systemets säkerhet. Individer bör även informeras om vilka tredje parter som har tillgång till information, deras rättigheter när det kommer till datatillgång och även hur de kan gå tillväga för att nyttja dessa (Hoepman 2014).

6. Control

Kontrollstrategin syftar till att individer vars data samlats in bör ha påverkan över hur personinformationen bearbetas. Denna strategi är en viktig motpart till informeringsstrategin då att informera om att personinformation samlats in saknar vikt om det inte även ges en viss kontroll över informationen. Denna strategi understryker vikten av att ge individer möjlighet att utöva sin rätt över sin personinformation i form av att se, uppdatera eller radera den insamlade personinformationen. Kontrollstrategin täcker även hur användare kan välja vilka system de vill använda och hur de kontroller vilken information som dessa system samlar in. Detta innebär att det även påverkar interaktionsdesignen av system då detta påverkar till vilken utsträckning som användaren ges kontroll över sin personinformation, till exempel som integritetsinställningar på sociala nätverk. Genom att ge användare kontroll över sin egen personinformation kan kvaliteten av personinformationen höjas då individer med större sannolikhet rättar eventuella fel i informationen (Hoepman 2014).

7. Enforce

Denna strategi syftar till att en integritetspolicy som uppfyller juridiska krav ska finnas och förstärkas. Detta är för att försäkra att det alltid finns en integritetspolicy och att den följs genom hela organisationens drift. Hur mycket integritet skyddas beror på policyn, minimikravet är alltid att den uppfyller juridiska krav men begränsas inte till det. Genom att förstärka integritetspolicyn så bör det finnas tekniska skydd mot att policyn bryts, detta innebär att ledningsstruktur som stärker policyn bör vara etablerat (Hoepman 2014).

8. Demonstrate

Den sista strategin kräver att en datakontrollant kan visa att organisationen uppehåller integritetspolicyn och uppfyller alla juridiska krav för integritetsskydd. Detta är specificerat i lagstiftning och kräver också att en kontrollant kan visa att det är implementerat och sätter krav på hur dataintrång hanteras (Hoepman 2014).

2.4 Teoretiskt ramverk

Viktiga omständigheter	Nyckelord	Litteratur
Digital integritet	Privacy by design Privacy by default Proaktiv design Holistiskt synsätt Integritet	Cavoukian (2009) Datainspektionen (2019) GDPR, (EU) 2016/679 Gürses et. al. (2011) Wylder (2003)
Informationssäkerhet	Åtkomstbegränsning End to end security Interna policys Enforce Confidentiality	Al Hamdani (2009) Agarwal & Agarwal (2011) Cavoukian (2009) Datainspektionen 2019) Dhillon & Backhouse (2000) GDPR, (EU) 2016/679 Hoepman (2014) Wylder (2003)
Informationsbehandling	Minimise data Anonymisering Transparency	Cavoukian (2009) Datainspektionen (2019) GDPR, (EU) 2016/679

	Inform	Gürses et. al. (2011) Hoepman (2014)
Användares rättigheter	Collection limitation Data limitation Purpose specification Use, retention and disclosure limitatiion	Cavoukian (2009) GDPR, (EU) 2016/679 Gürses et. al. (2011)
Ansvarsroller	Personuppgiftsansvarig Personuppgiftsbiträde Demonstrate	Datainspektionen (2019) Dhillon & Backhouse (2000) GDPR, (EU) 2016/679 Hoepman (2014)

Table 2.1: Teoretiskt ramverk.

3 Metod

3.1 Metodval

För att få en förståelse för det vi ville undersöka var det viktigt att få en teoretisk uppfattning av ämnet. För detta vände vi oss till tidigare studier och forskning kring ämnet och relaterade teorier. Då det vi valt att undersöka är ett relativt nytt ämne var det svårt att hitta forskning kring specifikt detta ämne och vi fick därför lägga fokus på teorierna och forskningen som lagt grunden till GDPR. För att undersöka det valde ämnet krävdes ytterligare undersökning.

Då vi ville förstå hur GDPR påverkat IT-konsulter, vilket är ett ämne som till stor del saknar forskning, valde vi att utföra kvalitativa intervjuer vilket Jacobsen (2002) anser vara lämpligt för att skapa större klarhet i ett oklart ämne. Jacobsen (2002) anser även att en kvalitativ metod är mest lämplig när vi vill utveckla nya hypoteser. En kvalitativ metod lägger vikt vid nyanserade svar, öppenhet och det unika hos varje uppgiftslämnare (Jacobsen 2002). Detta stämde väl in på vår undersökning och flexibiliteten av kvalitativa intervjuer möjliggjorde att utföra mer avslappnade intervjuer där vi kunde ställa våra frågor i en mer naturlig ordning istället för att ha ett förutbestämt frågeformulär.

3.2 Urval

Då vi valt att fokusera på IT-konsulter var det tydligt vilken arbetsroll de vi intervjuade bör ha. Utöver att individens arbetsroll är IT-konsult så sattes några andra kriterier upp. Individerna bör att arbetat aktivt både före och efter GDPR trädde i kraft, i flera separata projekt. Individerna bör arbeta på olika organisationer för att inte endast få insikt i en specifik organisations tillvägagångssätt. Ett annat kriterium var att individen bör ha uppfattning om organisationens generella strategi och standardlösningar för att få en mer övergripande insikt och inte projektspecifika omständigheter. Respondenterna presenteras i tabell 3.1 nedan.

Namn	Arbetsroll	Organisation	Intervjutyp	Längd	Appendix
Respondent 1	Konsultchef	It-konsultbolag, Business to Business, organisation 1	Telefon	26 minuter	A
Respondent 2	Back-end-konsult	It-konsultbolag, organisation 2	Videosamtal	34 minuter	B
Respondent 3	Frilanskonsult	Statliga myndigheter	Telefon	19 minuter	C

Table 3.1: Sammanfattning av intervjupersoner.

3.3 Intervju

I brist på möjlighet av personliga intervjuer utfördes samtliga intervjuer över telefon eller videosamtal. Dessa gjordes i lugn miljö och spelades in för att kunna bearbetas i efterhand. Samtliga intervjuer började med en presentation av vår uppsats, i vilket syfte intervjuerna utförs och att de kommer redovisas anonymt.

3.3.1 Intervjuguide

Intervjuguiden utformades utifrån det teoretiska ramverket för att förenkla analysering av empirin. Då vi använde oss av semistrukturerade intervjuer så blev intervjuguiden mer riktlinjer än fasta frågor. Detta med syfte av att kunna ställa följdfrågor, ge ett mer naturligt samtalsflöde och som stöd utefter behov. Intervjuerna följde därför inte intervjuguiden i alla situationer utan gav möjlighet till mer personliga svar. Intervjuguiden har även förbättrats mellan intervjuer då vi märkt att visa frågor inte var givande och att det fanns vissa delar som behövde mer fokus.

Digital integritet	• Är du bekant med Privacy by design? • Är detta något du anser har talats om i större omfattning efter GDPR trädde i kraft?
Informationsbehandling	• Lagrar ni mindre personinformation än ni gjorde innan GDPR trädde i kraft? • Har längden som ni lagrar personinformation minskat? • Anonymiserar ni personinformation till större grad nu än innan? • Hur informeras individer om hur och i vilket syfte deras personinformation samlas in? • Är det likadant i era tjänster?
Informationssäkerhet	• Hur går ni till väga för att se till att personinformation inte lagras eller ges åtkomst till obehöriga? • Har er organisations interna policys förändrats efter GDRP trädde i kraft? • Har säkerhetsaspekten av era tjänster behövt uppdatering för att uppfylla GDPR?
Användares rättigheter	• Hur har GDPR:s krav på användarrättigheter som till exempel att del av sin personinformation påverkat era tjänster? • Är dessa rättigheter något ni fått åtgärda själva eller har det tillkommit i era tjänster på andra sätt?

Ansvarsroller	• Vad har eran organisation för ansvar när det kommer till kundens databehandling? • Har GDPR ökat det ansvaret? • Försöker ni minimera det ansvaret och om detta är fallet hur går ni till väga?

Table 3.2: Intervjuguide.

3.4 Bearbetning

3.4.1 Transkribering

Efter att intervjuerna var genomförda började vi transkribera dessa. Vi spelade in samtliga intervjuer för att registrera hela samtalen, vilket enligt Jacobsen (2002) är idealet när det gäller kvalitativa metoder. Detta gjorde att vi kunde hoppa fram och tillbaka i intervjun utan att behöva hålla samma tempo som intervjun när den analyseras (Jacobsen 2002). Det möjliggör även kommentarer och understrykningar av viktiga stycken från intervjuerna vilket garanterar att ingenting glöms bort vilket är lättare hänt om analysen endast sker från inspelning (Jacobsen 2002). För att förenkla analysering av intervjuerna utelämnades enstaka upprepningar och tomma meningar från transkriberingarna.

3.4.2 Kategorisering

För att vidare förenkla analysering av transkriberingarna så kategoriserade vi dessa utifrån det teoretiska ramverket. Analysen kunde då utföras enklare genom att jämföra de kategoriserade transkriberingarna med litteraturen. Då vissa svar vidrörde flera kategorier så kan dessa svar återkomma i separata kategorier. Utöver det etablerade teoretiska ramverket uppstod svar som inte passade in ramverket, detta ledde till tillkomsten av en ny kategori och placerades under denna. Det är svar som vi, utifrån litteraturgenomgången, inte förutsåg men anser har en tillräckligt stor påverkan på studiens resultat och slutsatser för att vara relevant.

3.5 Etik

Vi började varje kontakt med intervjuperson genom att presentera studien, studiens syfte samt om de var intresserade att bli intervjuade och erbjuda deras kunskap. Utav de tio individer vi kontaktade ställde tre personer upp på intervju.

3.5.1 Inspelning

Samtliga intervjuer började med en samling etiska frågor. En av de första frågor som ställdes var om individen gav samtycke till att intervjun spelades in och senare transkriberades. Detta gav samtliga intervjupersoner samtycke till och inspelning startades inte fören det etiska frågorna hade ställts och besvarats.

3.5.2 Syfte

Samtliga intervjupersoner fick en presentation av vår studie och dess syfte för att ge dem en tydlig bild. I denna korta presentation försäkrades även intervjupersonerna om att intervjuerna endast kommer användas i syfte till denna studie och inte något mer. Detta anser Jacobsen (2002) vara viktigt för att individer fritt ska kunna välja om de vill delta i studien eller inte. Alla intervjupersoner erbjöds även att ta del av den färdiga studien för att följa upp.

3.5.3 Anonymitet

Inför alla intervjuer blev alla respondenter erbjudna att vara anonyma. Detta för att i det i många fall förekommer att individer inte vill svara om svaret kan kopplas till dem som personer (Jacobsen 2002). Då vi utförde en kvalitativ studie så är det enkelt att identifiera personer om deras information inte anonymiseras. Vi valde därför att utelämna information som namn, ålder, kön och vilken organisation de arbetar för. Detta gjordes för att det inte skulle falla några konsekvenser för de intervjuade och för att vi skulle få så ärliga svar som möjligt. Fokus vid denna studie var att få en förståelse för deras arbetsroll och inte individen i fråga vilket ledde till att vi valde att utelämna personinformation och fokusera på deras arbetsroller istället.

3.6 Validitet

De individer vi intervjuat har passat in i våra urvalskriterier och passade väl in i studien. Dessa anser vi vara relevanta till vår studie och valet av metod möjliggjorde ärliga svar med uppföljdsfrågor vilket Jacobsen (2002) anser vara relevant till en studies validitet. Trots att Jacobsen (2002) anser att personliga möten är att föredra i en kvalitativ uppsats var vi, i brist på möjlighet, tvungna att hålla samtliga intervjuer över telefon och videosamtal. Hade möjligheten funnits så hade vi utför intervjuerna genom personliga möten.

Samtliga intervjuer började med att respondenten frågades om det var okej att vi spelade in intervjun, vilket samtliga respondenter gav sitt samtycke till. Syftet med inspelningarna var att se till att inga svar missades vilket kan hända om man endast tar anteckningar. Efter intervjuerna så transkriberades de kort inpå för att de fortfarande ska vara färska i minnet och inte påverkas av våra egna tankar.

4 Empiri

Kapitel fyra redovisar resultaten från den empiriska undersökningen som vi avser vara relevanta till studiens syfte. Svaren från de kvalitativa intervjuerna är kategoriserade efter samma kategorier som litteraturgenomgång. Transkriberingar finns under Appendix A-C.

4.1 Digital Integritet

4.1.1 Proaktiv design

I intervjun med R2, som arbetar som back-end-konsult, berättar hen om att den aldrig hört uttrycket privacy by design men att konceptet är väldigt bekant. R2 beskriver hur integritetstänket är väldigt närvarande under hela livscykeln av data men att det inte alltid är huvudfokus. R2 uttryckte att:

”Hos de kunderna jag varit hos, så kan jag säga; ja det gör man absolut. Man har rätt omfattande frameworks kring hur man behandlar hela livscykeln av data, och när man bygger nya tjänster måste man ha det i åtanke från början.” (Appendix B:17).

R2 beskriver även hur det i många fall när organisationer bygger nya system är fokus på att bygga minimal viable product och att endast se till att det är GDPR-kompatibelt om det behövs.

R3 berättade att hen knappt är bekant med privacy by design och att det kom i samband med GDPR. R1 kände inte till privacy by design alls.

4.2 Informationsbehandling

4.2.1 Lagring av data

R1 berättade att GDPR inte påverkat mängden data de lagrar alls utan det enda som påverkats är att de är mer restriktiva med att data inte tas med från kunder. Hen anser även att det inte skett någon större förändring i hur systemen hanterar data. Att samtliga kundregister ser likadana ut och att det inte skett någon förändring. R1 uttrycker att de kanske har städat upp i sitt CRM-system men att det inte är särskilt stora förändringar där heller. Huvudförändringen har skett inom HR där de samlat all data i ett system och raderar den så fort den inte längre är nödvändig. Detta anser R1 kan komma att ändras när allt fallit på plats men att det i dagsläget inte har förändrats. R2 uttrycker även att hen inte sett någon minskning i mängd data som lagras utan endast i hur den lagras. Hen anser att det mer handlar om att vara innovativ om hur man lagrar data och att lagringen sker på ett mer ansvarsfullt sätt. R2 uttrycker även att mängden information som lagras bara ökar men att det måste lagras på ett mer ansvarsfullt sätt, så som anonymiseringslösningar. Utifrån de projekt som R2 varit del av har hen upplevt att många databaser och services har behövts städas upp och att man kan dra slutsatsen att det är väldigt mycket mer medvetet nu än tidigare. R2 beskriver även hur retention time, längden

man lagrar data, har begränsats med hjälp av standardtider så att så fort data skapas så är den inställd på att endast finnas under en viss period för att sedan raderas. Detta för att minska risk för läckor och kostnader för lagring. Detta anser R2 ha kommit med GDPR och blivit mycket vanligare sedan den trädde i kraft. Där R2 är anställd som utvecklare nu sätts även krav på att metadata, att den som skapar data måste definiera vad det är för typ av data. R3 anser att det är möjligt att det lagras lite mindre data men att den stora skillnaden efter GDPR trädde i kraft är att organisationer har koll på vad för information de lagrar. Hen berättar att där hen varit som konsult så ligger fokus på vilken information som lagras och var den lagras. Att organisationer kanske struntar i ovidkommande information men att den informationen som behövs måste lagras och att det är där fokusen ligger. Fokus ligger mer på var data lagras så att det går att ta bort den om det behövs och är möjligt och att begränsa eventuella skador som kan uppstå.

4.2.2 Anonymisering

R2 talar om hur många organisationer valt att applicera anonymiseringslösningar för att säkerställa säkerhet. Detta görs genom att identifiera vilken data som är känslig och sedan anonymisera den känsliga datan. Detta är dyrt att applicera då det kräver att infrastruktur implementeras. Hen berättar om ett projekt hen var på där de simulerade en data leak och försökte implementera en anonymiseringslösning vilket resulterade i att det var tvunget att läggas ner då det inte gick att utföra tillräckligt kostnadseffektivt. R3 uttrycker att organisationer kanske anonymiserar där det är möjligt men att fokus ligger på att kunna konstatera och hitta informationen. Hen har arbetat som konsult på statliga myndigheter och beskriver att anonymisering inte är ett val för dem. R3 berättar att statliga myndigheter måste kunna lagra och veta till vem personinformation tillhör men att det inte har samma vikt på den privata sektorn.

”När det gäller statliga sektorn där är det att antingen är du intresserad av personen eller också är du inte det och då har du ingen information.” (Appendix C:33).

Då R1 arbetar företag mot företag, där lagras inte personinformation på samma sätt och knappt alls. Där behövs inte information anonymiseras och de påverkas därför inte särskilt mycket.

4.2.3 Transparens och att informera

R3 beskriver hur det främsta sättet att informera användare om datainsamlingens syfte och individers rättigheter är genom hemsidor. Det görs genom disclaimers där det står att informationen lagras och i vilket syfte. Användare ska enligt R3 få en riktig och tydlig disclaimer där det tydligt står att informationen som användaren matar in lagras i deras interna system.

4.3 Informationssäkerhet

4.3.1 Åtkomstbegränsning

R2 nämner Access-control, hen förklarar att det är ett väldigt effektivt sätt för att låsa in data, eftersom när data skapas bör personen som äger data vara den som har tillgång till informationen, sen i sin tur bygga på flera lager och ge åtkomst till de som behöver datat, det kan ske

genom att till exempel en kollega skickar förfrågan för åtkomst, där de förklarar deras syfte med åtkomsten. R2 nämner att det finns många färdiga access management produkter, exempelvis Google cloud.

R2 fortsätter med att berätta att Access-control tekniken har funnits väldigt länge, men att med införandet av GDPR så tvingas alla till att använda det, tidigare har man bara markerat vilken data som är känslig och gett ett visst antal personer åtkomst till informationen beroende på vad för information det är, nu med införandet av GDPR har man introducerat mycket mer processer samt infrastruktur, hur man begär åtkomst och vem som ska få åtkomst, man loggar allt på ett annat och mer utförligt sätt.

R3 som mestadels arbetat för myndigheter berättar att de för det mesta förlitar sig på deras egna IT-organisationer, alltså sköter de själva lagringen samt vem som ska få åtkomst till känslig data, hen uttrycker dock att de flesta använder Office365 för mail och att det finns GDPR-information i mailen som skickas, det skyddas naturligtvis av Google eller någon av de leverantörer som har den typen av webbaserade system. R3 nämner att deras handläggningssystem för det mesta skyddas internt via deras brandväggar och informationssäkerhetssystem. R1 förklarar att de använder sig utav ett behörighetssystem, de som har tillgång är cheferna och respektive underordnade, det har varit så även innan GDPR. De har sekretess så att man till exempel inte ska kunna se allas löner samt HR-uppgifter utan det är styrt hierarkiskt.

4.3.2 Interna policys

R1 berättar att sättet behandlingen av de uppgifter som de behandlat tidigare inte har ändrats sedan GDPR har implementerats, den enda skillnaden R1 anser har skett är att det skett en förändring i deras avtal, där det står att de inte får plocka med data som är känslig och att GDPR finns, men i självaste systemet har det inte skett någon teknisk förändring:

”Förändringen är att vi har avtal numera som liksom talar om att vi inte kan plocka med oss data och att vi är mer restriktiva med data och att det finns GDPR. Systemen har inte ändrat sig” (Appendix A:54).

R2, beskrev hur olika organisationer implementerar skilda lösningar beroende på hur de tolkar lagen, R2 fortsatte med att berätta att deras interna policy har ändrats på det sätt så att alla måste förstå sig på åtkomstbegränsningssystemet som de använder som finns i deras cloud-provider.

Vi ställde frågan om den interna säkerhetspolicyn ändrats sedan GDPR trädet i kraft, R3 svarade att införandet av GDPR har lett till förändringar i deras interna säkerhetspolicy, när vi sedan frågade om det har ändrats på något särskilt sätt, svarade R3 att det handlar om att man efter införandet av GDPR hela tiden måste vara medveten om vad det är för data man lagrar, och vilken data som är GDPR-information och vad som inte är det, även hur man ska hantera GDPR-data, det är den delen som har förtydligats i deras interna säkerhetspolicy.

4.3.3 Tekniska åtgärder

R3 beskriver utvecklingen av den tekniska aspekten för informationssäkerhet, vi frågade om det skett någon förändring, med tanke på att GDPR har införts, R3 påstår att det inte har skett någon förändring, förutom att tekniken ständigt utvecklas och det införs nya uppdateringar och förbättringar, något som inte är så unikt, då nästan all teknik ständigt utvecklas, en utveckling som R3 nämner är att med hjälp av GDPR kan de spåra om en av deras användare försöker komma åt obehörig data, innan handlade det mer om ansökningsnummer eller registreringsnummer, men nu får man även tänka på GDPR-informationen.

R2 berättade hur informationssäkerheten som bör implementeras för att uppfylla GDPR har konserverat i höga kostnader för organisationer, hen tar upp en jobbsituation där hens kund körde data leak på Hadopp och försökte utveckla en anonymiseringslösning, som resulterade med att de fick lägga ner, eftersom de inte kunde uppfylla kraven då de krävdes för mycket resurser, de tekniska åtgärderna varierar alltså beroende på hur mycket resurser olika företag har då det både kostar mycket och det krävs tid för att implementera de nya tekniska åtgärderna.

R2 förklarade även hur anonymisering har blivit till en populär lösning som många företag använt sig utav:

”Många olika företag har olika implementationer, och vad många valt att göra är att köra en sådan anonymiserings-lösning där man kollar på vilken data är känslig, om de är känsligt så anonymiserar vi det. Det får ju en teknisk konsekvens, då det kan vara dyra operationer man gör när man anonymiserar och måste få ganska mycket såhär servicen och infrastruktur på plats” (Appendix B:139).

Vi frågade R1 om det skett förändringar i deras system efter införandet av GDPR, R1 menar att det inte har skett någon förändring och att deras system ser likadant ut, men hen nämner att det kan bero på att GDPR fortfarande är nytt och inte implementerats helt ännu.

4.4 Användares rättigheter

R1 förklarade att de nya rättigheterna från GDPR, inte har gjort någon större skillnad i deras system, för att de jobbar b2b, R1 menar att de som de har affärer med, inte skulle vilja bli bortglömda.

Vi frågade R3 hur GDPR nya rättigheterna för användare har påverkat hen när det skett en implementering av system, hen förklarade för oss att den största konsekvensen har varit att det kostat mycket att korrigera, eller utveckla nya lösningar.

R3 fortsatte med att berätta att det inte har påverkat alla lika mycket, då myndigheter kan böja på reglerna:

”Men jag tror att för statliga myndigheter har det varit lättare för där behöver man inte följa reglerna fullt ut. Det här med att man kan bli glömd, du kan ju försöka att bli glömd hos försäkringskassan så får du se. Det går liksom inte. Så att statliga myndigheter har det nog lite lättare än vad privata har i det avseendet. Jag tror även att det är så, eller det är så att böterna som de kan dela ut är lägre för statliga myndigheter än för privata.” (Appendix C:93).

R3 utryckte sig om vad hen tycker om de nya rättigheterna, hen anser att rätten till att bli bortglömd kan bli till en svår utmaning, då det inte är lätt att rensa någon från ett register som är gammalt, det kräver resurser, tid och mycket pengar. R3 säger att de flesta har koll på vad som bör göras, men att många ligger efter och inte är hemma när det kommer till utförandet.

R2 berättade att innan GDPR införde de nya rättigheterna, så fanns det en del saker som olika företag aldrig gjort innan, till exempel så nämner hen hur ”rätten att bli glömd” inte fanns i system tidigare, då det kostar för att utveckla en lösning för att uppfylla kraven, och även om man innan GDPR hade utvecklat ett system som uppfyller rätten att bli glömd så hade det i den stunden inte adderat något värde för företag.

4.5 Ansvarsroller

4.5.1 Personuppgiftsansvarig

I intervju med R2 beskriver hen att ansvaret för data som lagras ligger på kunden som lagrar den. Hen berättar att om en kund har anställt ett konsultbolag för att implementera en lösning så faller ansvaret för data och eventuella böter på kunden. Konsulter som arbetar hos kunder brukar få en kort kurs kring deras databehandlingspolicy som konsulterna måste följa. Ansvaret faller även då på kunden och konsult bär inget legalt ansvar då böter döms å företagsnivå och inte individnivå och konsulten arbetar på kundens företag. Även R3 uttrycker detta. Hen förklarar att om en organisation tar in konsulter så är organisationen ansvarig för det konsulterna gör. Konsulter skriver dock vanligtvis på ett sekretessavtal vilket även täcker GDPR och i det avseendet så bär även konsulten ett visst ansvar. Om en myndighet använder en tjänst så kan de aldrig peka på den tjänsten och säga att ansvaret ligger på dem. Det är organisationen som äger datan och anställer konsulten som är ansvarig för datan och när konsulten lämnar kunden så har den inte längre något ansvar. R3 berättar att på samma sätt så kan en organisation som använder sig av molntjänster aldrig lägga över ansvar på leverantören utan det är alltid organisationen som äger datan som är ansvarig.

”Som konsult kan man inte åka dit för något utan man gör det som kunden säger att man ska göra, rätt eller fel.” (Appendix C:154)

4.5.2 Datakontrollant

R1 uttrycker att ifall de skulle utsättas för kontroller så har de inga etablerade processer för att följa upp eller kontrollera att GDPR följs. Organisationen har inte heller implementerat en intern roll för detta. Ifall det skulle vara så att en kund hörde av sig om detta så utreds händelsen men det finns inga etablerade kanaler, roller eller processer för detta.

4.6 Övriga påverkningar

4.6.1 Avtal

R1 uttryckte att den största påverkan GDPR haft på organisationen är avtalsrelaterad och att organisationen måste upprätta nya avtal med alla kunder och leverantörer. Alla har sina olika avtalsformer och jurister som ska vara med i processen och det har lett till att alla avtal inte är på plats än. Dessa avtal, uttrycker R1, inte är särskilt prioriterade utan att andra saker går före.

”Men vi har ju inte avtalat med alla kunder än utan vissa tycker ju att det här kommer långt ner på listan över saker som behöver göras. Alltså helt enkelt att komma igenom våra avtals-former.” (Appendix A:82).

5 Analys och diskussion

I kapitel fem diskuteras empirin utifrån det teoretiska ramverket som presenterades i kapitel två. Detta kapitel syftar till att analysera samband och skillnader mellan empirin och det teoretiska ramverket.

5.1 Digital integritet

5.1.1 Proaktiv design

Cavoukian (2009) uttrycker hur design bör vara proaktiv och inte reaktiv för att skydda individers digitala integritet. Hon anser att privacy by design inte väntar på att risker materialiseras utan arbetar förebyggande. Privacy by design bör också sträva efter att leverera den högsta graden av integritet. Om en individ inte utför något så bör deras information vara skyddad, utan att individen behöver utföra något. Privacy by design bör även vara integrerat i designen från första början och inte läggas till i efterhand. Detta bör göras med hjälp av etablerade standarder och ramverk (Cavoukian 2009). R2 håller till stor del med om detta och beskriver hur integritetstänket varit närvarande redan från början i projekten hos de kunder hen varit konsult hos. Hos dessa kunder berättar R2 även om hur den finns etablerade och omfattande ramverk som hanterar hur data ska behandlas genom hela systemets livscykel. Även R1 har märkt av det proaktiva tänket. Det har inte påverkat R1 och dess arbete i samma utsträckning och nämner ingenting om ramverk eller integritetstänk. Den stora skillnaden för R1 är att konsulterna på organisationen har fått en utbildning för att vara informerade om uttryck och vad de innebär. R1 nämner till exempel hur utvecklare har slutat med förifyllda formulär vilket grundas i privacy by default. Det proaktiva tänket är närvarande i olika grader utifrån svaren från respondenterna. R2 målar upp en mer utförlig bild där det proaktiva tänket är högst närvarande och det finns etablerade ramverk medan R1 endast märkt av en skillnad i utbildning.

5.2 Informationsbehandling

5.2.1 Datalagring

Den första privacy by designstrategin som Hoepman (2014) presenterar syftar till att organisationer bör minimera lagringen av data. Genom att minimera datalagring så minskar organisationer risker vid dataintrång och att data inte lagras utan syfte. Även Gürses et. al. (2011) uttrycker vikten av att minimera datalagring men även att limitera insamling av den för att skydda individers integritet. Cavoukian (2009) talar även om att minimera datalagring och insamling i sina grundprinciper men uttrycker även vikten av att specificera syftet, begränsa användningen, lagringstiden och avslöjandet av personinformation. Även Al-Hamdani (2009) anser att användbarheten av data är en central aspekt att ha i åtanke när organisationer lagrar information. R1 beskriver att mängden data de lagrar inte har minskat och att sättet de hanterar data inte har påverkats särskilt mycket alls efter att GDPR trädde i kraft. Ingen större förändring har skett utöver att de centraliserat lagringen av deras HR-system och att de nu är mer

noga med att data raderas när den inte längre är nödvändig. Detta går i linje med principen att begränsa användningen och lagringstiden av personinformation men strider mot samtlig litteraturs syn på minimering av datalagring och Hoepmans (2014) strategi om att separera databehandling och datalagring. R1 påpekar dock att detta kan komma att ändras när de kommer längre fram i GDRP-processen. Även R2 berättar att hen inte sett någon minskning i datalagring utan att det bara ökar och att det istället handlar om hur organisationer hanterar den. Det handlar om att hantera personinformation på ett mer ansvarsfullt sätt där R2 anser anonymisering vara ett av det vanligare tillvägagångssättet. Sedan GDPR trädde i kraft har det blivit vanligare med begränsade lagringsperioder. Detta appliceras med hjälp av standardtider där data raderas efter en viss tid vilket går i linje med Cavoukians (2009) syn på begränsningen av lagringstid. Där R2 arbetar nu sätts även krav på att metadata måste finnas, där det definieras vad det är för typ av data som lagras, vilket tydliggör datans behandlingssyfte och stärks av Cavoukians (2009) princip om syftesspecifikation. Även R3 ser att på de organisationer där hen har varit konsult så har mängden data som lagras inte minskat efter GDPR trädde i kraft utan att fokus ligger på vilken information som lagras och var detta görs.

5.2.2 Anonymisering

I Hoepmans (2014) fjärde privacy designstrategi beskriver hur personinformation bör sammanfogas till stora samlingar med lite detaljer utan att påverka användbarheten. Om den sammanfogas till tillräckligt stora grupper med få detaljer så blir den mindre känslig. Genom detta kan information nästan inte kopplas till en specifik individ och skyddar på så sätt individers integritet. Detta är något som R2 anser att många organisationer valt att göra genom anonymisering och på så sätt säkerställa säkerhet och integritet. Det utförs genom att identifiera känslig data och sedan anonymisera den. R3 anser att organisationer anonymiserar om det är möjligt men att det viktiga är att konstatera och hitta informationen. R3 har huvudsakligen arbetat som konsult i den statliga sektorn och berättar att de inte har möjlighet att anonymisera personinformation. Statliga myndigheter måste kunna lagra och identifiera personer med hjälp av personinformation och kan därför inte anonymisera den. Business to business konsulter påverkas inte på samma sätt enligt R1. De lagrar knappt personinformation och behöver därför inte anonymisera.

5.2.3 Transparens och informering

Både Hoepman (2014) och Cavoukian (2009) anser att individer informeras om hur deras information behandlas och transparens som vitala aspekter. Båda uttrycker att individer bör informeras om hur deras data behandlas och i vilket syfte. Hoepman (2014) anser att individer som använder sig av ett system ska informeras om vilken data som bearbetas och i vilket syfte. R3 anser att det främsta och vanligaste sättet att informera användare om vilken data som bearbetas och varför är genom disclaimers. R3 samstämmer med Hoepman (2014) och Cavoukian (2009) om att användare ska informeras tydligt att informationen användare matar in lagras och i vilket syfte.

5.3 Informationssäkerhet

5.3.1 Åtkomstbegränsning

Agarwal & Agarwal (2011), förklarar i CIA-triaden att data bör skyddas genom att ha åtkomstkontroll samt rättigheter. De personer som har åtkomst till känslig data ska vara begränsade och de får ej använda känslig data på ett inkorrekt sätt, R2 håller med CIA-triaden då de använder sig utav åtkomstkontroll i form av färdiga access management produkter som deras utvalda cloudproviders erbjuder. R3 arbetssätt är också i enighet med CIA-triaden då de har åtkomstkontroll i deras interna system, men jämfört med R2 som använder cloudproviders, så skiljer R3 sig en del, skillnaden är att R3 för det mesta arbetar inom myndigheter som vanligtvis förlitar sig på deras egna IT-organisationer vilket betyder att de själva ansvarar för deras åtkomstkontroll, annars är det samma princip då både R2 och R3 använder sig utav åtkomstkontroll med rättigheter. R1 använder sig av ett behörighetssystem, vilket betyder att även de använder sig utav åtkomstkontroll.

I RITE modellen nämner Dhillon & Backhouse (2000) nya aspekter som en utvecklande modell till CIA-triaden, bland dessa aspekter så förklarar de i Integrity-aspekten att organisationer bär på känslig data, så det är väldigt kritiskt för verksamheterna att kontrollera vilka det är som har åtkomst till den känsliga informationen, alla våra respondenter har varit i enighet med denna aspekt då de använder sig utav åtkomstkontroll där de utvärderar vem som bör vara behörig innan de ger åtkomst till data som är känsligt.

5.3.2 Interna policys

Hoepmans (2014) sjunde privacy designstrategi,”Enforce”, innebär att en integritetspolicy som uppfyller juridiska krav ska finnas och förstärkas. R1 berättar i intervjun att de efter införandet av GDPR har de framställt ett avtal som informerar om GDPR, vilken data de inte får ta, och att de allmänt måste vara mer restriktiva med data på grund av GDPR. R1 är alltså i enighet med ”Enforce” startegien som Hoepman (2014) framtagit. I vår intervju med R2 förklarade hen, att de utöver att informera om GDPR i deras interna policy, så har de även adderat hur de ska använda sig av till exempel deras åtkomstbegränsningssystem. Även R3 förklarade för oss att efter införandet av GDPR, så har de infört uppdateringar i deras interna policy som förklarar GDPR. i deras interna policy har de tagit med vad för data som ska lagras, hur GDPR-data ska hanteras och vilken data som är GDPR-information och vad som inte är det. Alla respondenters svar tyder på en uppdatering i den interna policyn efter trädde i kraft vilket Hoepman (2014) uttryckt och lagt vikt i.

5.3.3 Tekniska åtgärder

Hoepman (2014) nämner ”Hide” som en av privacy designstrategierna. Denna strategi säger att genom att gömma personinformation, blir risken för att personinformationen ska utnyttjas mindre. R2 berättade i intervjun att anonymiseringslösningar är något som blivit populärt efter införandet av GDPR. De verksamhet som använder sig av anonymisering är i enighet med Hoepmans (2014) Hide-strategi, då den känsliga informationen döljs via anonymiseringsprocessen.

Även om anonymisering har blivit populärt och används flitigt av verksamheter, så finns det fortfarande många som inte använder sig utav det, R2 berättade om ett projekt hen haft, där de försökte implementera en anonymiseringslösning, men resurserna räckte inte till, alltså har inte alla verksamheter de resurser som krävs för att uppfylla strategierna Hoepman (2014) tagit fram.

R3 förklarade att hen för det mesta arbetat som konsult för statliga myndigheter, där säger R3 att anonymisering inte är ett alternativ, för att statliga myndigheter måste lagra samt veta vem personinformationen tillhör, men hen nämner att det inte är lika viktigt för privata verksamheter att hålla reda på exakt vem informationen tillhör, alltså appliceras inte Hoepmans (2014) strategi på samma sätt när det gäller myndigheter, då de i många fall måste veta vems data de behandlar.

5.4 Användares rättigheter

(Datainspektionen 2019) förklarar att med införandet av GDPR så har det tillkommit nya rättigheter för användarna. Användarna ska ha rätt till att ta del, uppdatera samt radera personuppgifter som handlar om användaren i fråga, Al-Hamdani (2009) antyder på detta i hans Diligence model, där är en av aspekterna ”Authenticity”, som menar att information ska vara korrekt, överstämmande och genuin. För att uppnå aspekten Al-Hamdani (2009) framtagit bör användare kunna ta del av och redigera information som är felaktig. Med införandet av GDPR så har användarna rätt till just detta. Även Hoepman (2014) stärker detta med kontrollstrategin som syftar till att ge användare kontroll över sin egen personinformation och att användarna ska ha rätt till att ta del av, uppdatera och radera sin information.

GDPR ger användarna rätten till att bli bortglömd (Datainspektionen 2019), men enligt R1 används inte denna rättighet där hen arbetar, hens argument till varför de inte har påverkats av denna nya rättighet är för att de jobbar business to business. R1 menar att de som de har affärer med inte har behov av att bli bortglömda. R2 förklarar att de nya rättigheterna för användare har haft en stor påverkan. Att kunna bli raderad har inte funnits tidigare då det inte adderat något värde för organisationen. R2 menar att de nya rättigheterna har orsakat höga kostnader för verksamheter, på grund av korrigering och utveckling som har utförts för att verksamheterna ska uppnå kraven. R3 utryckte sig angående att myndigheter inte behöver följa de nya rättigheterna från GDPR lika noga som privata verksamheter, som ett exempel tog han upp Skatteverket, han menar att man inte kan begära att bli raderad hos statliga myndigheter, därför följer de inte reglerna fullt ut.

5.5 Ansvarsroller

5.5.1 Personuppgiftsansvarig

GDPR uttrycker att man kan dela upp ansvaret för informationsbehandling i två parter, personuppgiftsansvarig och personuppgiftsbiträden. Den personuppgiftsansvarige är organisationen som samlar in och äger data och personuppgiftsbiträden är organisationer som behandlar datan som tredje part (Datainspektionen 2019). Det finns alltid ett personuppgiftsbiträde som behandlar organisationers data och det är upp till denna att det sköts korrekt. Detta

stärker även Hoepman (2014) med den sista av hans privacy designstrategier. Dhillon & Backhouse (2000) beskriver hur RITE-modellen lägger vikt i att anställda är medvetna om ansvaret i deras arbetsroll. R2 berättar att ansvaret för data som lagras ligger på kunden som äger den och att om kunden har anställt ett konsultbolag så faller allt ansvar och eventuella böter fortfarande alltid på kunden. Konsulter får vanligtvis en kort utbildning om kundens databehandlingspolicy och att den måste följas. R2 uttrycker att ansvaret alltid faller på kunden och att konsulterna därför inte bär något ansvar för datan och dess behandling. Även R3 uttrycker att organisationer som anställer konsulter är ansvariga för vad konsulterna gör. Då konsulter vanligtvis skriver på ett sekretessavtal och bär därför ett visst ansvar i det avseendet. Om en myndighet använder sig av en tjänst så kan den aldrig lägga något ansvar på tjänsten. Organisationen som äger informationen är ytterst ansvarig och när en konsult lämnar en kund så har konsulten inte längre något ansvar. Samma principer gäller organisationer som använder molntjänster, även där faller ansvaret på organisationen och inte leverantören av molntjänsten.

5.5.2 Datakontrollant

Lagstiftningen kräver att en datakontrollant kan visar att juridiska krav uppfylls och att kontrollanten kan demonstrera att det är implementerat i organisationen (Hoepman 2014). Hoepmans (2014) sista privacy designstrategi uttrycker vikten av att det finns en datakontrollant. I R1:s organisation finns det inga etablerade processer för att följa upp eller kontrollera att juridiska kraven är uppfyllda. Det saknas även en implementerad intern roll för detta. Ifall ett dataintrång skulle ske finns det inga etablerade processer eller roller för att hantera detta utan det utreds utifrån incidenten.

5.6 Övriga påverkningar

Den största påverkan GDPR haft på R1 och dess organisation har varit kraven på nya avtal med kunder och leverantörer. Dessa avtal har dock inte varit prioriterade utan har fallit ner på listan av saker som måste utföras. R1:s organisation arbetar business to business och har därför inte påverkats så mycket av GDPR då de flesta aspekter faller på deras kunder eller systemleverantörer, det enda som varit märkbart har varit krav på nya avtal.

5.7 Reflektion av intervjupersoner

De personer vi har intervjuat arbetar alla inom olika delar av IT-konsultbranschen på den svenska marknaden. Resultatet berör därför huvudsakligen den svenska marknaden och kan se annorlunda ut i andra länder då alla länder har egna implementeringar av GDPR. Då de arbetar i olika konsultroller och på olika organisationer så påverkas de av olika aspekter av GDPR på olika sätt. Resultatet bör därför inte ses som fakta utan som en insikt i praktiken.

6 Slutsats

Resultatet från denna studie visar inte en entydig bild. Hur GDPR har påverkat konsulter skiljer sig utifrån hur konsulten arbetar. Då konsultarbetet sträcker sig från statliga myndigheter till business to business så skiljer sig påverkan markant. GDPR:s krav framträder mest påtagligt för konsulter i rollen som utvecklare. Kraven som ställs på systemet har förändrat utvecklingsprocessen där integritetstänket är mer närvarande genom hela utvecklingsprocessen. Detta skiljer sig beroende på om arbetet sker på den privata eller statliga marknaden. Den privata marknaden har hårdare krav och hårdare möjliga straff. Den statliga sektorn påverkas inte lika mycket då de kan undgå vissa väsentliga delar av GDPR:s krav och kommer lindrigare undan ifall dessa inte följs. Minst påverkan har varit på business to businesskonsulter. Då dessa knappt handskas med personinformation så har GDPR inte burit med sig några större förändringar.

Resultatet visar även att informationssäkerhet inte har förändrats markant sedan GDPR trädde i kraft. De säkerhetskrav som GDPR ställer har redan varit på plats och har inte krävt någon anpassning. Den aspekten som påverkats mest har varit interna policys där de huvudsakligen blivit striktare kring integritet och personuppgiftsbehandling men det har inte tillförts några nya tekniska verktyg för att förstärka dessa policys.

Något som är konsekvent genom empirin är synen på ansvar. Konsultens roll är att uppfylla kundens krav och bär inget ansvar för data som behandlas. Under inga fall anses konsulter vara personuppgiftsansvariga. Konsulterna arbetar under kundens ansvar och det enda personliga ansvaret de bär är att följa kundens riktlinjer och ramverk. När konsulten lämnar kunden och utfört sitt arbete bär de inte längre något ansvar för vad som händer med personuppgifterna som behandlats eller kommer behandlas på organisationen. Konsulterna arbetar på så sätt i en slags gråzon där de inte behöver oroa sig över personuppgiftsansvar.

Resultatet visar en splittrad bild av hur prioriterat att uppfylla GDPR:s krav är. På ena sidan har GDPR varit ett stort projekt som många lagt ner stora resurser, både tid och pengar, för att följa. På andra sidan prioriteras GDPR lågt på prioriteringslistan, kunder vill endast något som fungerar och endast uppfylla GDPR om det behövs. Då det skiljer sig så mycket från kund till kund leder detta till att det även skiljer sig bland konsulter.

6.1 Förslag till vidare forskning

Då det finns väldigt få studier inom detta område så föreslår vi att det utförs vidare forskning. Vi skulle vilja se vidare studier där fokus ligger på specifika konsultroller för att få insikt i rollspecifika påverkningar. Vi föreslår även vidare forskning med ett större antal konsulter av olika arbetsroller för att få vidare förståelse för att påverkningarna som GDPR haft på de olika arbetsrollerna.

Appendix A

IL – Intervjuledare

R1- Respondent 1

IL: Hur bekant är du med konceptet privacy by design?

R1: Privacy by design... inte alls.

IL: Inte alls? okej

R1: Haha det borde jag kanske ha men nej det känner jag inte till.

IL: Okej, det är ett uttryck som används i GDPR men inte är specifikt satt som krav utan används som ett sätt att uppfylla GDPR:s krav men det är inte specifikt uttryckt att det ska vara just det. Jag tänkte bara stämma av det lite i förväg

R1: Ja men alltså GDPR är något som finns liksom men skulle inte säga att vi är experter på det på något sätt och vi sitter väl mer. men fråga du på så får vi se.

IL: Ja men det är nästan bättre så för hade ni varit experter så hade det inte varit lika intressant att fråga er. Jag tänkte börja med att fråga lite om informationsbehandling. Lagrar ni mindre personinformation än ni gjorde innan GDPR trädde i kraft?

R1: Lagrar vi mindre information... nu tänker du på kunder eller?

IL: Ja det blir väl i form av kundinformation.

R1: Alltså vi har ju avtal och sånt där och det är samma saker, det är ganska oförändrat egentligen. egentligen utan några större förändringar utan att vi har ett appendix som behandlar GDPR i våra avtal kan man säga. Det är det som egentligen är förändring men jag kan inte säga att hanterar information på ett annat sätt, det kan jag inte säga.

IL: Okej, det här kanske jag borde frågat först men jag slänger in det lite här emellan. Er organisation, när det kommer till kundens databehandling, för ni levererar en tjänst till kunden, har ni något ansvar för kundens databehandling som sker inom den levererade tjänsten eller är det helt på kundens sida?

R1: Alltså vi ansvarar ju inte för kundens data överhuvudtaget. det vi har är restriktioner i hur vi hanterar kundens data. Vi får liksom inte ta med oss data ut eller så utan det är hos kunden och det är deras ansvar.

IL: Jag förstår, och GDPR har inte påverkat det ansvaret på något sätt?

R1: Nej det kan man inte säga.

IL: Skönt

R1: Eller mer än att vi är mer restriktiva med det här att vi inte tar någonting med oss eller vi, ja, vi vet ju om det här på ett annat sätt kan man säga.

IL: Jag förstår

R1: Det är inte så att vi snodde med oss data tidigare. utan allting ligger hos kunden, kundens maskiner och så.

IL: Jag förstår. och när det kommer till tjänster, utvecklar ni egna tjänster eller erbjuder ni färdiga tjänster?

R1: Alltså vi implementerar standardsystem, ERP och sånt, det är ju M3 som är Infor och Dynamics som är Microsoft så det är deras produkter som implementerar så vi bygger ingenting själva på det sättet även fast vi naturligtvis kan göra det. Lägga till saker och det. Det är i princip de två leverantörer som ansvarar för produkterna kan man säga.

IL: Okej, så ni håller inget ansvar när det kommer till hur information lagras i systemen överhuvudtaget?

R1: Nej, inte mer än hur man kan konfigurera och så naturligtvis. Där kan vi ju prata om olika sätt att hantera olika uppgifter men det är ändå trots allt kunden som ansvarar och i grunden är det inte vårt system utan vi bara konsultar på det så att säga.

IL: Jag förstår, kan ni se någon större skillnad i hur systemen behandlar information efter GDPR har trätt i kraft? Har det förändrats något på den fronten?

R1: Hm, nej det kan jag inte se där heller. Alla dom uppgifter som vi haft har vi haft tidigare också och inte förändrat. Alltså det är kunduppgifter, om man tänker sig ett kundregister då, dom finns ju kvar och där är inga förändringar gjorda i dom. Nej det tycker jag inte, ingen större skillnad. Förändringen är att vi har avtal numera som liksom talar om att vi inte kan plocka med oss data och att vi är mer restriktiva med data och att det finns GDPR. Systemen har inte ändrat sig.

IL: Avtalsrelaterat, är det grundat i interna policys?

R1: Ja

IL: Och det är då den stora förändringen kan man säga från innan till nu

R1: Ja och sen har man ju naturligtvis informerat ut till själva konsultkåren och så vidare vad det är som gäller, det har ju funnits med tidigare, tänket att vi inte tar data från kunder och sprider ut eller tar med oss. Där kan jag inte se någon skillnad, mer än att vi informerar och att folk ska veta om.

IL: Så den interna policyn ser ungefär likadan ut?

R1: Ja. Sen har man ju det här som är ett avtal mellan kund och leverantör nu med GDPR. Det är mer det som har varit det stora jobbet. Alla kunder och alla leverantörer ska vi upprätta dom har avtalen med och alla har ju sina avtalsformer och sina jurister som ska titta på det här

så det är där det stora jobbet är och alla avtal är inte klara heller utan det pågår och pågår och pågår och diskuteras.

IL: Spännande att det nästan blir mer fokus på det juridiska än den tekniska delen av det.

R1: Ja, ja.

IL: Det är lite intressant då GDPR specificerar just databehandlingen.

R1: Ja, men så kan jag säga att det kanske förändrar sig när allting är på plats och att det blir mer tryck just på, ja, hur det appliceras och hanteras men fram tills nu har inte vi känt av något sånt alls just i databehandling.

IL: Skulle du säga att alla är up to speed nu med GDPR? Är alla där dom ska vara eller finns det fortfarande organisationer och kunder som inte riktigt kommit till det stadiet att vara helt GDPR compliant?

R1: Eftersom att alla avtal inte är på plats än så, det var ju ett väldigt tjatande för, det var ett år sen det gick igång va?

IL: Exakt

R1: Men vi har ju inte avtalat med alla kunder än utan vissa tycker ju att det här kommer långt ner på listan över saker som behöver göras. Alltså helt enkelt att komma igenom våra avtalsformer. Det är liksom snarare där det ligger, det är inte riktigt avtalat på alla håll kanske.

IL: Om man bortser från själva avtalen och kollar på den faktiska principen bakom tjänsten ni levererar och sättet ni utför, skulle du säga att dom stora ERP systemen som ni levererar, är dom helt GDPR compliant? Är dom uppdaterade, har dom gått igenom någon stor uppdatering eller någon slags uppdatering för att det ska uppfylla GDPR eller är det samma systemversion?

R1: Nej det är snarare hur man hanterar datan som är GDPR.

IL: Så det ansvaret ligger hos kunden och inte på systemet?

R1: Ja, alltså jag kan säga som jag har märkt GDPR delarna är ju när vi söker folk. Alltså i anställningsförfarandet så får man ju inte längre hålla på och skicka runt ansökningshandlingar och sånt där längre där flera tittar på det. Nu har man alla dom här sakerna i ett system och där ligger dom så man skriver inte ut och skickar inte runt utan det ligger där och hanteras och tar bort när processen är avslutad, om dom blir anställda eller inte anställda så försvinner liksom alla betyg och cv och alla anställningshandlingar och sånt. det är något jag märkt av.

IL: Så det är nästan bara internt, liksom HR-mässigt som GDPR har förändrat?

R1: Ja det är HR-mässigt och det är ju internt hos oss och inte hur vi jobbar med kunderna.

IL: Det är väl mer övergripande oavsett organisation och inte specifikt för it-konsultbolag tänker jag?

R1: Ja men det är ändå något som jag som chef känner av att där är något som är viktigt att kolla på. Så att inte personliga papper försvinner iväg.

IL: Jag förstår, det är ju också en ganska stor insikt i hur GDPR har tvingat folk förändra sättet dom hanterar information i allmänhet.

R1: All korrespondens ligger liksom i ett rektryteringssytem, HR-system.

IL: Jag kör vidare lite, en stor del av GDPR är ju individens rättigheter. Att man har rätt till att del av sin information, uppdatera den om den är felaktig eller kräva att den ska tas bort. Är det något som är nytt i era tjänster och system eller har det redan funnits sen innan?

R1: Det har funnits sedan innan. Dom register som finns i ERP system är ju liksom ett kundregister och ett leverantörsregister, det är inte så att det är kunder som vill plockas bort eller leverantörer som vill plockas bort utan är oftast långa förhållanden och det är business to business, företag till företag, så det är inte så mycket personer i dom här systemen som kunder köper utan det är business to business och det är inte riktigt samma fokus på det. Så det är inte mycket personuppgifter, det är någon referens någonstans men i övrigt är det företag till företag. Så där är ju en skillnad.

IL: Vad intressant. När man ser på GDPR och läser det så får man intrycket om att det ska göra jättestor förändring så det är ganska intressant att se att det inte påverkar så mycket.

R1: Kanske HR-system, som sagt, tror jag det kan vara såna förändringar på. Så är det det första man nämner med rekrytering och sådant. Men sen löner och sånt har ju alltid varit på det här sättet. Slutar man så slutar man och då är det bara att plocka bort den.

IL: Ja det är klart. Har ni något särskilt sätt att gå tillväga för att personinformation, internt blir det då, inte lagras eller ges åtkomst till fel personer? Hur ser ni till att någon som inte har med den här anställningsprocessen att göra till exempel inte kan ta del av själva ansökan?

R1: Det är ju behörighetssystem. Så dom som har tillgång är ju cheferna och respektive underordnade då. Det är som normalt, och har funkat så alltid och är ingen förändring efter GDPR. Det är den sekretessen det är, att man inte kan se allas löner och HR-uppgifter utan är strypt hierarkiskt. Och sen naturligtvis dom som jobbar på hr. Så har det alltid funkat.

IL: Jag förstår. Det är ganska intressant för nu när jag sitter här, jag har ju utformat en intervjuguide.

R1: Kan du hålla den? haha

IL: Ja det är lite det som är spännande att jag nu inser att utifrån teori och litteratur och allting man grundat i så får man en annorlunda bild än du målar upp just nu. Då får man ju bilden av att GDPR ska påverka nästan alla delar av IT-system generellt.

R1: om man skulle beställa som en privatperson så är det lite annorlunda. Om man jobbar mot att beställer varor på webben så kanske du vill bli bortplockad men det är ju inte dom systemen vi har. I ERP systemen är det mer fasta kunder och fasta leverantörer man har och business to business.

IL: Jag förstår. Om du skulle spekulera lite kring om man skulle leverera ett system som hanterar kunduppgifter, som ett CRM-system till exempel, tror du att det har skett en stor förändring i hur ett sånt system hanterar uppgifter eller fanns det best practices som var ganska lik?

R1: I CRM-system så fins det ju lite personliga uppgifter och sånt. Alltså kontaktpersoner egentligen. Där finns ju lite sån data. Jag tror vi har tvättat lite där. Det är ju redan idag behörighet på sånna saker så det är inga stora förändringar där heller. Jag känner inte att vi har några starka påtryckningar på att kunna plocka bort. Om en kund ringer som ansvarar för något specifikt som vill veta vad vi vet om honom i vårat CRM-system, det händer inte. Inga problem med att göra det, det har vi kunnat göra tidigare också.

IL: Så man skulle kunna säga att dom kraven GDPR nu ställer, när det kommer till databehandlingen, nästan varit best practices? Att det redan varit vedertagna sätt att hantera data?

R1: Ja det har ju funnits tidigare, det är klart vissa områden, just på CRM så kanske man behöver, där kan ju finnas personlig information. Jag säger inte att vi har det, jag tror inte speciellt mycket sån information utan det är mer information om företaget. Vilka versioner dom kör och naturligtvis vilka kontaktpersoner som finns. Det är i regel bara namn, det är inte så att vi har personuppgifter eller spelar personen golf, det är inget sånt utan är bara, jaha det är kalle svensson han ansvarar för ERP-systemet hos Cloetta eller något. Det är den typen och inget mer, vi har inte adresser på dom utan det är företagets adress.

IL: Så bara kontaktuppgifter helt enkelt.

R1: Ja mailadress och sånt, telefonnummer. Men det är liksom företag och inte hem till personen.

IL: Så lite summa summarum, skulle du säga att GDPR inte påverkat er så mycket?

R1: Nej inte mer än avtal och sådär och att vi naturligtvis att vi inte riktigt vet vad som kan hända om myndigheterna skulle dyka upp och hitta någonting som vi inte har tänkt på. Jag vet inte, jag har inte lagt mycket tid på det utan det är avtalsformerna, att få till alla avtal mellan kund och leverantör.

IL: Och det är det enda som egentligen har förändrats?

R1: Ja, det är det. Vi har även haft en liten utbildning för alla konsulter så att dom vet, ja, hur vi ska förhålla oss och sådär.

IL: Den utbildningen, har det varit något nytt i den eller har den varit mer av principsak att nu när det träder i kraft så påminner vi?

R1: Det finns väl lite nya begrepp och aktuellt. Ska se här.

IL: Men det är inget nytt i interna policys eller något sånt?

R1: Nej det kan jag inte säga att det är. Ska ta fram en och titta lite. I utbildningen så fick man ett antal frågor. Man skulle veta vad ett data breach är för något, ett hyfsat nytt begrepp.

IL: Så det var mer för att fylla på metodologin än något annat?

R1: Ja, det är lite kring utveckling också. Att man inte ska ha förifyllda sånna här boxar när man utvecklar något. Med GDPR och så.

IL: Ja exakt, om dom inte är förifyllda i att man inte lagrar något så är det ju jobbigt.

R1: Och sen är det right to information och right to access och sånt som är viktigt att känna till vad det kan innebära.

IL: Okej, nämns det i utvecklingen eller är det bara begrepp man ska känna till?

R1: Nej det är mer om vi kommer åt data i vårt system så ska dom kunna vet vem hos oss som haft access till data och sådär. Så det har ju varit en utbildning men jag känner inte att det är något som ändrats. Kanske inte var så mycket som man trodde från början. Det jag själv tänkte var ju mer alla mail som skickar fram och tillbaks.

IL: Som jag förstått det, jag ska inte kalla mig för expert, men beror väl lite på vem som ansvarar för mailservern så är den intern så blir väl det en fråga om GDPR också.

R1: Nej jag har inte märkt något alls. Vi har inte fått någon restriktion på att man inte får lagra mail eller något sånt.

IL: Men är det ni som hanterar den mailservern?

R1: Nej det är Microsoft.

IL: Då ligger det ju på dom.

R1: Men dom har ju ingen aning vad vi har på den.

IL: Nej det är klart. Vad intressant.

R1: Har det gett någonting?

IL: Absolut, att få insikt i att det inte påverkat så mycket är ju en stor insikt i sig.

R1: Men som sagt, det är i sin linda fortfarande tror jag. Alltså att det mest varit att nu ska detta igång och nu ska vi ha avtal mellan kund och leverantör. Det är egentligen det som har hänt. Sen kommer det kanske en massa kontroller och grejer som vi inte riktigt känner till. Man kan inte säga att vi har någon speciell process på att följa upp eller kontrollera att vi följer och inte gör saker och ting.

IL: Så ni har inte implementerat någon slags ansvarsroll internt för det?

R1: Inte mer än den vanliga sekretessen när man jobbar med kunders data.

IL: Så ifall det skulle hända att någon kom och ställde frågor, vad händer då?

R1: Det är ju om någon kund har några frågor om dom som jobbat med just deras data och sådär. Så får ju naturligtvis plocka in dom och utreda vad det är som hänt. Om någon har kommit i kontakt eller någonting. Det händer aldrig, trots att vi jobbar med lite banksystem och sånt, finansiella saker som borde vara mycket GDPR i och så. Men nej, det har inte kommit.

1

Appendix B

IL – Intervjuledare

R2 – Respondent 2

IL: Hur bekant är du med begreppet Privacy By Design?

R2: Jag har fakstiskt inte hört begreppet tidigare, men det låter verkligen som en sån här design for GDPR grej, att vi i processen har med kundens data i åtanke.

IL: Ja det är något som nämns i GDPR men inte specifikt uttrycks som ett krav, det är som ett tips att kolla på, och grundar sig på att man integrerar privacy-tänket från början av utveckling och ej lägger på det i efterhand, det är hela konceptet egentligen.

R2: Hos de kunderna jag varit hos, så kan jag säga; ja det gör man absolut. Man har rätt omfattande frameworks kring hur man behandlar hela livscykeln av data, och när man bygger nya tjänster måste man ha det i åtanke från början. sen kanske det inte är det man fokat på direkt, för att när man bygger nya tjänster, handlar det om att bygga minimal viable-product, och få saker att funka, se till så det är GDPR-kompatibel om det behövs. Så försöker man göra så lite arbete som möjligt kring det så att man uppfyller kunden framework eller blir GDPR-compliant.

IL: När du arbetar som konsult, har du levererat ett färdigt system, eller är ni på plats och utvecklar hos kunden?

R2: Färdiga system har vi inte levererat till någon vad jag har förstått. GDPR kom ju väldigt fort, och det är även en lag, så att vad jag förstått från de ställen jag varit på och mina kollegor så kan företag tolka GDPR på olika sätt, så olika företag gör olika mycket inom detta område, sen så kom det ingen produkt på marknaden som var tillräckligt flexibel fort nog för att kunna anpassas till många kunder eller framförallt stora kunder. Så företagen har byggt egna lösningar. Större kunder har nästan alltid en cloud-provider, finns en massa olika alternativ, med införandet av GDPR har man varit mycket i kontakt med cloud-tjänsterna för att få deras tjänster att samspela med GDPR, på så sätt har ju dom utvecklat sina produkter. Så nu kan man börja se att det börjar komma mer standardlösningar på cloudtjänster för GDPR. Snart kommer det nog vara att egna system inte utvecklas men det var väldigt mycket så i början. Folk har väldigt olika approach och olika lösningar så tills man satt någon typ av standard i branschen så utvecklar man egna grejer.

IL: När man utvecklar systemen, kan man se att informationslagring har minskat?

R2: Hos dom kunderna jag har varit så har det inte minskat. Det handlar mer om att vara innovativ kring hur man gör det, då använder man mycket anonymiserings-lösningar och liknande. Så nej det där ökar bara. Det är bara att man får lagra det på ett mer ansvarsfullt sätt.

IL: Hr det skett någon förändring i lagringen?

R2: Jag har arbetat som konsult i 2 år, när jag började jobba så var GDPR väldigt hett, typ alla IT-projekt handlade enbart om GDPR för det var det man var tvungen att lösa. Det blev plötsligt prio ett för i princip alla, så jag har inte riktigt sett världen före GDPR som konsult, men vad jag har sett, är att under mina 2 år har jag fått städa upp ganska många dataset och services som inte varit GDPR-compliant och från dom kan man ändå dra slutsatsen att det har blivit extremt mycket mer medvetet nu. Som en konsekvens av detta pratar man mycket om retention-time, alltså hur länge man får lagra data. Nu har man en standardtid, så när data skapas så sätts en den default till att leva i 90 dagar och efter 90 dagar så raderas den. Det är då för att minska risk för dataläckor, även kostnader för både lagring, och beräkning av data. Som jag förstår så är detta något som kommit med GDPR och växt mycket större.

IL: Skönt att höra att de har skärpt sig när det gäller lagring.

R2: Ja, det verkar så. Hos de kunderna jag har varit hos har verkligen skärpts till, och det jag hört från mina kollegor är att det har skärpts riktigt hårt.

IL: Har det varit påtagligt när du jobbat?

R2: Ja det har det ju, då jag jobbat med GDPR-utveckling, jag gör ju inte det just nu, där jag är just nu. När jag bygger grejer på Organisation X, måste man alltid följa de här GDPR-ramverken som är just hur länge man får lagra data, vem som kommer åt data, vad för typ data. Man samlar mycket mer metadata på data, alltså data som beskriver data, om man skapar dataset, måste man själv gå igenom och säga det här är en adress osv, så man har full koll på vad det är för data. Det tror jag inte dom gjorde där innan, eller jag är rätt säker på att dom inte gjorde det innan GDPR. Det märks absolut.

IL: Du nämnde access control och åtkomst. Är access control huvudrestrektionen?

R2: Ja det skulle jag säga, access control är ett väldigt effektivt sätt att låsa in data. Det är alltid någon som producerar data, någon som äger datan. Så när man skapar data är det effektivt att den som skapat data by default är den som ska ha tillgång till data och sen bygger man flera lager av GDPR-services som tillåter dina kollegor att komma åt data. Då kan man kolla vad kollegorna har för syfte med att kolla upp data, vad det syftet är, om de kan komma åt det direkt beroende på hur känslig datan är. Med sån här identity access management produkter, till exempel Google cloud har färdiga sånna produkter, även AVS har färdiga produkter. Så när man skapar data där kan man direkt själv begränsa vem som kommer åt det, men sen kan man ha flera lager ovan på det, så att man själv som företag säger denna data är väldigt känsligt. Om en person vill komma åt det måste personen begära åtkomsten och tillhandhålla ett syfte för att komma åt den, så att det är absolut detta som är huvudprodukten för att stänga ner data och göra det mer säkert så alla inte kommer åt allt.

IL: Vad har skilt sig från innan till nu? Är det någon skillnad i interna policys? För systemet har haft ungefär samma möjlighet att ge och ta ifrån åtkomst av data.

R2: Det är som du säger, tekniken har funnits hur länge som helst, det är bara det att nu med GDPR så tvingas alla till att använda den, och använda den på ansvarsfullt sätt, och det kan man göra i olika granulariteter. Tidigare när man låste ner standardprodukter sa man bara ”ja denna data är känslig, vi ger bara tillgång till ett antal personer”. Nu har man introducerat mycket mer processer och infrastruktur om hur man begär åtkomsten och vem som får den, alltså att loggar allt på ett helt annat sätt.

IL: En förändring i interna policyn alltså?

R2: Ja exakt, jag kan visa hur vi gör, till exempel såhär, vi kör ju Google cloud så all vår data och alla våra tjänster körs alltid på Google cloud, så de lagrar våran data tillsvidare. De har färdiga access manament, där jag själv kan låsa ner all data jag skapat, om jag skapat data på Google storage och du vill komma åt den så kan jag lägga till dig här, Theo… select row, sen kan jag kolla storage, sen kan jag se till så du bara kan läsa min data, detta har funnits väldigt länge, men nu med GDPR ovanpå det här bygger man ytterligare tjänster och ytterligare säkerhetslager. Hur vi gör på Organisation X, så om man skapar sin data i big-query, sen i schemat i big-queryn kan man lägga till descriptions i alla fält, i name här, så följer vi ett format där vi säger att här står det användarID, det kommer sedan mappa den här tabellen automatiskt något ännu striktare än det jag satt på GCP. User interface söker upp data, sen får man begära åtkomst därifrån, beroende på vad jag mappat som dataägare, så kommer det bli olika strikt, om den kommer fatta om det ej är känslig data, då får begäraren access direkt och har den accessen i 90 dagar och om jag vill ha access igen så måste jag förnya det. Men om man mappat mot något superkänsligt måste personen som vill komma åt det skriva syfte till varför de vill ha den känsliga data, sätta syften man definierat i förhand, sen skickat det vidare till en legal-grupp som godkänner det eller även min manager som är ansvarig för mig som skapat datat, man har byggt tjänster ovanpå de klassiska tjänsterna, men även processer ovanpå det för att göra det mer GDPR-compliant. Det handlar mycket om att… grundidén är väldigt enkel, det är så att de som inte använder eller behöver datat ska inte se datat eller exponeras av det, därför desto fler som ser datat desto större risk är det att de läcker. Överallt vi lagrar data, oavsett om det är Big-query, filer eller pubsub så har vi GDPR-tjänster och lagar ovanpå det, som vi kopplar samma access request-modul. Så fort jag vill ha data så loggar jag bara in där och söker upp det och requestar så funkar det väldigt snyggt, men det är väldigt mycket jobb att bygga det här och få de på plats. Det investeras mycket pengar för att få det att funka. I framtiden kommer dessa lösningar standardiseras och erbjudas på ett bättre sätt, till exempel GCP eller AVS. Alla dessa cloud providers är amerikanska bolag som kanske inte tog GDPR jätteseriöst så det kommer väl mer och mer.

IL: Hur ser det ut med ansvaret för data, är det hos er eller hos Google som provider? Ifall det skulle hända en data breach hos er, skulle det gå ut över er organisation eller skulle det ansvaret ligga hos Google?

R2: Det är en svår fråga... Det beror på vad det är för breach, det beror på vad som hänt, var ifrån de tagit sig in, har de tagit sig in via Google eller Organisation X? Det är nog en väldigt

vital fråga men det är kunden som lagrar datan som har de yttersta ansvaret då de väljer Google som tredje part så i slutändan blir de dom som bär ansvaret. Men jag har inte läst legala dokumenten från GDPR så jag vet inte riktigt hur det är. Men det är intressant.

IL: I GDPR står det att de som hanterar personuppgifterna är personuppgiftansvariga, de har de yttersta ansvaret då, alltså är kunden ansvarig då de behandlar data, men de kan anställa en tredje part som personuppgiftsbiträden, då blir det tredje parten som utför behandlingen, då blir ansvaret tillsammans på något sätt.

R2: Ja, men säg till exempel att kund A har anställt ett konsult bolag, de får böter men böterna faller ej på konsultbolaget alls, även om de är konsultbolaget som implementerat lösningen, för att det är kunden som bär yttersta ansvaret, för att när jag går till en kund, då får jag en utbildning där för att följa deras databehandling-policys, de brukar vara en onlinekurs man går på ungefär 2 timmar där man går igenom allt och sen får acceptera det för att få jobba där, Det enda jag märker som konsult är att självklart följer jag policyn de sätter samt försöker aktivt förbättra dom, det är lite konsultens roll att komma in och bygga god kundrelation, vilket man inte gör om man tänjer på deras regler, då är man väldigt noga som konsult att följa, men huruvida om det sker dataläcka eller sådär vet jag inte riktigt om jag som konsult egentligen bär något legalt ansvar då det ligger på kunden. Man döms ju till böter på bolagsnivå och inte individnivå.

IL: Det nämndes lite kort i en tidigare intervju om avtalsklausuler så jag tänkte om det kanske ligger något där?

R2: Jag har ju inte kommit så långt i min karriär så att jag fått se dem här klausulerna och sitta med i dem förhandlingarna. Jag är lite mer i monkey-stadiet och gör som jag blir tillsagd haha.

IL: Skönt! Vi pratade ju om åtkomst vilket är en säkerhetsprincip man implementerar för den mänskliga faktorn men kan man se att den tekniska säkerhetsaspekten har förändrats? Har organisationer lagt mer krut på teknisk säkerhet?

R2: Man kan ju implementera GDPR på lite olika sätt, det är en lag som tolkas, det är upp till kunden hur de vill göra. Många olika företag har olika implementationer, och vad många valt att göra är att köra en sådan anonymiserings-lösning där man kollar på vilken data är känslig, om de är känsligt så anonymiserar vi det. Det får ju en teknisk konsekvens, då det kan vara dyra operationer man gör när man anonymiserar och måste få ganska mycket såhär servicen och infrastruktur på plats. Den ena kunden jag va hos körde en data leak på Hadoop och försökte bygga en sådan anonymiseringslösning, vilket mer eller mindre slutade med att man fick lägga ner allt för dom kunde inte bygga upp det tillräckligt effektivt då det kostade för mycket att köra alla jobb och såhär. Det kan vara en teknisk säkerhetsaspekt som har ändrats, där har det skett en teknisk konsekvens och utmaning. Eller var det det som var frågan?

IL: Informationssäkerhet är ju ett ganska brett ämne. Det handlar ju både om anonymisering och åtkomstrestriktioner. Jag tänkte mer specifikt på hårdkodade lösningar, som brandväggar och liknande?

R2: Det är inte riktigt min domän faktiskt, men jag tror inte det har ändrats så mycket med brandväggar och säkerhet då IT-säkerhet alltid varit viktigt. Brandväggar håller man på mycket med när man kör onPrem och har sina egna servar och kör på sin egna datacluster och såhär, jag skulle inte säga att det är otrendigt, men trenden går ju absolut att man bara lägger ut all till exempel hos Google eller AVS och de sköter det åt en mycket. Att man har infrastruktur as a service som ingår, slippa konfigurera och sånt där, men de jobbar ju otroligt mycket med säkerhet dessa här cloud providers. Jag tror all data vi har är krypterad i typ fyra lager hos Google.

IL: GDPR har gett en del rättigheter till slutanvändarna, har det varit en påtaglig förändring? Har det varit något som behövts uppdateras eller har det redan varit på plats?

R2: Nej, där jag har varit är det något man absolut inte gjort tidigare, framförallt den här ”rätten att bli bortglömd” det är ingen som haft det på plats, det adderar ju inget värde till företaget egentligen, det är inget man lagt pengar på för att implementera, men det är något man fått lägga mycket resurser på och få på plats. Det är något som konsultbolag varit ganska glada över, det har skapat mycket jobb.

IL: Så det är något konsulter går in och själva gör?

R2: Jag skulle vilja säga att detta är något typiskt som man anställer konsulter för. När GDPR kom så var det ingen som visste riktigt hur man skulle hantera det och hur man skulle göra, och då när man som ett företag inte har den kompetensen inhouse, och inte heller har resursen att säga till anställda att släppa det de gör och satsa på GDPR i ett år. Det gör man inte riktigt, då anställer man gärna konsulter för att göra detta tidsbegränsat, men även i hopp om att konsulter har nätverk. Så om man går till till exempel Accenture som har en halv miljon konsulter och ganska många tusen kunder, så kanske man får en god idé om hur man ska lösa GDPR. Det är en riktigt typisk konsultuppgift. Det var någon fråga om att minimera ansvaret, det är ganska intressant. Det kan nog vara lite olika hos olika konsultföretag. Jag skulle vilja säga att man inte vill minimera ansvaret, som konsult är det som en affärsrelation mellan konsultbolaget och kunden, när man kommer in som konsult hos en kund vill man stanna där så länge som möjligt, man vill även växa kunden så det kommer in mer folk. Det låter ej som att skjuta ifrån sig ansvar och ha strategier att försöka minimera sånt som kunden uppenbarligen tycker är jobbigt, det låter inte som en särskilt god affärsstrategi, som konsult tar man det ansvaret och lite till för att bygga upp en god affärsrelation.

IL: Det är spännande, väldigt logiskt, att höra med tanke på litteratur vi läst tidigare där bilden kan skilja sig lite.

R2: Det är i alla fall min take, vi har aldrig försökt skjuta ifrån oss något ansvar, ser vi att kunden tycker något är jobbigt vilket man sett att GDPR är och såhär så ser man det som en möjlighet för att få mer uppdrag och projekt.

IL: Nice, det var det när det kommer till frågor, stort tack för att du ställde upp.

Appendix C

IL – Intervjuledare

R3 – Respondent 3

IL: Hur bekant är du med begreppet Privacy By Design?

R3: Inte sådär jättemycket skulle jag vilja säga, det uttrycket är inget som jag har använt själv.

IL: Jag förstår, är det något som du hört innan GDPR, eller kom det i samma våg?

R3: Nej, det kom nog i samband med GDPR i så fall, det är inget uttryck som jag använder egentligen och det är inget som jag har hört speciellt mycket gällande GDPR heller egentligen. I så fall har jag nog hört någon svensk översättning.

IL: Okej, jag tänkte bara stämma av lite. När du har varit ute i konsultrollen, har det varit som utvecklare, eller har det varit för att implementera färdiga lösningar?

R3: Det har varit både och, främst färdiga lösningar, men även design lite grann, jag är ingen utvecklare själv men design utav lösningar, framförallt hur man ska hitta den informationen som man behöver hitta system, vilka ändringar som behöver man göra och vilka loggar behöver man leta i.

IL: Skulle du påstå att man lagrar mindre personinformation nu efter att GDPR har trätt i kraft än man gjorde innan? Att man i sina lösningar minimerar sin personinformationslagring?

R3: Det är möjligt att man kanske lagrar lite mindre, men det man definitivt gör nu för tiden är att ha koll på vilken informationen man lagrar på ett annat sätt. Jag tror mer att man har fokuserat, iallafall där jag varit inblandad, på vilken information man har och var man har den. Att man skulle lagra mindre, ja det är möjligt att man i vissa lägen struntar i information som är helt ovidkommande men den information man behöver måste man ändå lagra och det är det man fokuserat på. Att hitta vart man lagrar vad så att man kan dels ta bort det om det skulle behövas, om det ens är möjligt, vilket det inte är i alla system. men iallafall begränsa dom skador som kan uppstå gällande personlig information.

IL: Anonymiserar man denna data på något sätt?

R3: Där det går så har man nog gjort det, men jag skulle vilja hävda att det som jag har sett, det är mer att man kan konstatera och att hitta informationen. Där det går att anonymisera, absolut, men myndigheterna jag varit mer inblandad i är det inte ett val egentligen. Du måste ju veta vem personen är om det är information om den personen, du behöver lagra liksom. På den privata sidan kan jag tänka mig om det är annonser och grejer är det kanske inte lika viktigt att ha all information om en person i fråga. När det gäller statliga sektorn där är det att

antingen är du intresserad av personen eller också är du inte det och då har du ingen information.

IL: Hur informeras individerna? Får de reda på i vilket syfte deras information lagras?

R3: Ja, det är främst via hemsidorna naturligtvis, där dom lägger upp dom här disclaimerna som dom ser. Om man registrerar något i något system så ska man ju få en disclaimer på webben. Alltså nu ska du vara medveten om att vi lagrar det här. Det skulle jag säga måste vara den absolut vanligaste metoden.

IL: Den klassiska Cookie bannern då?

R3: Ja egentligen men det behöver ju inte vara en cookie utan det kan ju vara att om du lägger in något i ett system. Cookien har ju egentligen sessionsinformation, det är ju cookiens roll. Att om du går tillbaka till den webbsidan så ska webbsidan komma ihåg att du har varit där tidigare. Jag tänker mer på att om du skriver in någonting som faktiskt lagras i något system bakom då ska du få en riktig disclaimer att nu kommer vi lagra ditt data i våra interna system.

IL: Det avslutar det lilla blocket om hur information behandlas. Jag kör vidare. När det kommer till informationssäkerheten, hur går man till väga för att se till att personinformation inte ges åtkomst till obehöriga?

R3: Det är nog väldigt olika hur folk väljer att göra men min åsikt och det som jag har sett, och åter igen så rör mer egentligen myndigheter än privata företag, så är det väl att man skyddar den viktiga informationen så gott det går. Det är väldigt många statliga myndigheter fortfarande som inte kör molnbaserade lösningar. Det innebär att du har du ju mesta delen av informationen i ditt egna system, i den egna datahall. Jag tror att myndigheter iallafall fortfarande förlitar sig på sin egen IT-organisation om man nu har någon för att skydda informationen. På det viset menar jag att då har man koll på informationen själv. Man lägger den inte i molnet om man inte måste. Men däremot använder väl dom flesta Office365 för mail och det finns väl GDPR-information i nästan vartenda mail som skickas och den informationen är naturligtvis hos Google eller någon av dom leverantörerna som har den typen av webbaserade system. Vad det gäller handläggningssystem så skyddas det mesta internt på myndigheterna. Det är ju brandväggar och informationssäkerhetssystem som man själv har. Man följer sina egna riktlinjer. Det gäller ju inte bara GDPR och personinformation egentligen utan det gäller ju all information som är icke-offentlig.

IL: Har den interna säkerhetspolicyn ändrats sen GDPR trädet i kraft?

R3: Ja det skulle jag säga att den har. Dom interna säkerhetspolicys har ändrats i och med GDPR, ja.

IL: På något särskilt sätt som sticker ut?

R3: Nej, jag skulle vilja säga att det har med hur man nu för tiden hanterar, man måste ju hela tiden vara medveten om vad som är GDPR-information och vad som inte är det. Så att det är väl det man har försökt förtydliga i sina interna policys. Hur man ska hantera den formen av information. Det är nog olika på olika företag, absolut. Men det är väl från hur du designar system till vad som händer när du avslutar systemet. Det är hela processen, vad det gäller just den informationen som har med personer att göra. Det är väldigt svårt ska jag säga för det finns många gamla system. Man hade inte en tanke på GDPR och kanske inte ens på PUL när dom där systemen byggdes och det är inte jättelätt att ändra på alla sådana grejer och det finns

säkert hur många system som helst där man helt enkelt inte har koll på det här egentligen. Man försöker så gott man kan.

IL: När man kollar på, som du nämnde med brandväggar, den delen som handlar om den rena tekniska informationssäkerheten, har den ändrats?

R3: Jag skulle vilja säga att den är samma som innan, däremot så kommer hela tiden nya funktioner i dom här säkerhetstjänsterna. Det som är hett nu är det här med informationssäkerhet och att man ska kunna spåra om någon försöker kopiera information som innehåller till exempelvis ett personnummer, då ska systemet larma. Det är lite nyare funktioner som kommit, med hjälp av GDPR så kan man faktiskt då spåra sådana grejer som om någon försöker göra något med personnummer och förhindra det rent tekniskt. Det är klart att den typen av förändringar kanske mer sker just nu. Förut så var man kanske inte så fokuserad å GDPR-informationen utan på ett ansökningsnummer eller ett registreringsnummer, det som var viktigt för det företaget. Nu får man även börja fundera på GDPR informationen.

IL: Du nämnde tidigare att ta bort information, att alla inte riktigt kan det. Hur skulle du vilja säga att GDPR:s krav på användarrättigheter, exempelvis som att ta del av deras information, radera sin information eller uppdatera den, har det påverkat system som du implementerat?

R3: Ja det har blivit ökade kostnader kan jag säga, eftersom man måste designa och korrigera de systemen man har för att kunna uppnå kraven. Det har ju varit väldigt stökigt. Men jag tror att för statliga myndigheter har det varit lättare för där behöver man inte följa reglerna fullt ut. Det här med att man kan bli glömd, du kan ju försöka att bli glömd hos försäkringskassan så får du se. Det går liksom inte. Så att statliga myndigheter har det nog lite lättare än vad privata har i det avseendet. Jag tror även att det är så, eller det är så att böterna som de kan dela ut är lägre för statliga myndigheter än för privata. Eftersom jag har mest erfarenhet av statliga myndigheter så har man inte behövt tänka lika mycket på den grejen, att man ska kunna bli glömd där, eftersom det finns undantagsregler för det. Jag skulle vilja säga att det är ett stort problem, att rensa någon i ett register som är gammalt är inte det lättaste. Det kräver resurser, tid och pengar, för att åstadkomma det. Dom flesta har nog koll på vad dom behöver göra men att det är många som ligger efter och inte är hemma vad det gäller själva utförandet.

IL: Tekniska möjligheten att rensa en ut ur ett system, är det något du har själv varit med och slipat in eller har det tillkommit på annat sätt i systemet?

R3: Jag har varit inblandad i några projekt där man har utvecklat system själva och då har man fått gå in med konsulter eller egna resurser och redigera dom här sakerna. I vissa fall har man valt att inte göra det, utan man har bara konstaterat, att här skulle man behöva göra något men det får vi göra när vi har tid och pengar.

IL: Och i dom färdiga systemen, då är själva producenten som fixar det?

R3: Precis och det är ju upp till dom hur dom tycker att dom är GDPR-compliant eller inte. Alla säger väl att dom är det, men jag tror inte att alla är det egentligen. Jag tror inte att om du eller jag skulle vilja att vårt Hotmailkonto försvinner helt och hållet och att all information vi har där bara skulle försvinna över en natt, jag tror inte ens att Microsoft grejar det för det finns ju kvar i back-uper. Någonstans finns informationen det är bara det att den inte syns. Det där med att man ska rensa bak, jag menar om du har back-uper 5 år tillbaka i tiden då finns ju den där informationen i dom back-uperna och jag tror inte att det är många som har system

som går in och rensar i back-uper till exempel. Det är ju liksom, systemet okej men det går ju att få tillbaka informationen om man vill.

IL: Ja, det är omfattande. När det kommer till ansvar, har du som konsult något ansvar när det kommer till kundens databehandling i ditt konsultuppdrag?

R3: Jag skulle vilja säga att i normalfallet så får man skriva på en sekretessförbindelse och det gäller även GDPR-grejerna. Det är en sak man normalt sett får göra när man kommer in som konsult på ett ställe. Om dom som man är hos har sådan information naturligtvis. Det brukar man få göra och det är klart att man har ett ansvar.

IL: Har GDPR ökat det ansvaret eller är det mer specifikt att det här är något som också behövs tänkas på?

R3: Om du är ett företag och ska göra ett system eller en förändring i ett system, då är det alltid det företaget som är ansvarig. Tar du in konsulter är du ändå ansvarig för det dom gör. Man kan aldrig peka på någon annan, om du är en myndighet som använder Office 365 för din mejl, då kan du aldrig peka på Microsoft och säga att det är deras fel och det är dom du ska straffa. Du har skyldighet för ditt eget data, alltid. I princip så är det du som har ansvar för det som konsulterna gör. Som konsult har man i det avseendet inte så mycket ansvar. När du går därifrån och har gjort ditt då har inte du något ansvar längre som konsult.

IL: Då är man lite frisagd?

R3: Egentligen så är man det för det är företaget som äger informationen och är ansvarig för den, inte vad någon konsult har gjort. Och det gäller även dom här molntjänsterna, hävdar jag, att har du data hos en molntjänst då är det du själv som fortfarande är ansvarig. Så om den där molntjänsten släpper ut allt det där datat och har det öppet för alla att se och skickar det vidare och säljer informationen till folk som skickar ut reklam så är det ändå ditt ansvar och inte den målntjänsten ansvar.

IL: Jag kan tänka mig att det är svårt att säga att det är molntjänstens ansvar med tanke på att, antagligen så har ju den molntjänsten andra kunder också där det inte händer så då får man väl se det som att om en organisation, som använder till exempel GCP, läcker ut massa data. Då kan man ju inte peka på GCP för det är hur många andra som också använder det där data inte läckt ut.

R3: Ja, så att det är alltid du som är ansvarig för din information. Man kan aldrig lyfta över det ansvaret på någon annan tyvärr. Även om du har köpt tjänster av någon annan. Det blir svårt. Böterna hamnar hos företaget, inte hos molnleverantören om du har molntjänst.

IL: Är det något du vill tillägga om hur du som konsult har märkt att GDPR har förändrat för dig?

R3: Jag skulle vilja säga att man tänker mer på personlig information nu för tiden. Det skulle jag säga att man gör. Det är ändå ägaren av datat, det företaget som har den här databasen eller tjänsten som har hela ansvaret. Som konsult kan man inte åka dit för något utan man gör det som kunden säger att man ska göra, rätt eller fel. Sen kan man ju naturligtvis vara väldigt påläst om GDPR och säga att nej sådär kan ni inte göra för då är ni inte GDPR-compliant men jag skulle säga att om du är en ren GDPR-konsult så behöver du nog inte tänka så mycket utan det är företaget som har beställt jobbet som ska ha tänkt redan.

159 IL: Okej det var nog det, Tack så mycket för intervjun!

1

Referenser

Agarwal, A. & Agarwal, A., 2011. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, Volym 1, pp. 257- 259.

Al-Hamdani, W. A. (2009, September). Non risk assessment information security assurance model. In *2009 Information Security Curriculum Development Conference* (pp. 84–90). ACM.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada, 5.

Crossler, Robert and Posey, Clay (2017) "Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem," Journal of the Association for Information Systems: Vol. 18 : Iss. 7 , Article 2.

Datainspektionen (2019a). Anmälda personuppgiftsincidenter 2018: Datainspektionens rapport 2019.1

Datainspektionen (2019b). Dataskyddsförordningen. Hämtad 20 juli från: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningen---full-text/#K4

Datainspektionen (2019c). De registrerades rättigheter. Hämtad 22 juli 2019 från: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/de-registrerades-rattigheter/

Datainspektionen (2019d). Inbyggt dataskydd och dataskydd som standard. Hämtad 14 juli 2019 från: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/inbyggt-dataskydd-och-dataskydd-som-standard/

Datainspektionen (2019e). Personuppgiftsansvariga och personuppgiftsbiträden. Hämtad 13 juli 2019 från https://www.datainspektionen.se/lagar--regler/dataskydds-forordningen/personuppgiftsansvariga-och-personuppgiftsbitraden/

Datainspektionen har inlett en granskning av Klarna (2019f). Hämtad 12 juli 2019 från: https://www.datainspektionen.se/nyheter/datainspektionen-har-inlett-en-granskning-av-klarna/

Datainspektionen inleder granskning av åtta vårdgivare. (2019g). Hämtad 12 juli 2019 från: https://www.datainspektionen.se/nyheter/datainspektionen-inleder-granskning-av-atta-vardgivare/

Datainspektionen inleder sin tredje tillsyn kring 1177 Vårdguiden. (2019h). Hämtad 12 juli 2019 från: https://www.datainspektionen.se/nyheter/datainspektionen-inleder-sin-tredje-tillsyn-kring-1177-vardguiden/

Dhillon, G. & Backhouse, J., 2000. Information System Security Management in the New Millenium. Communications of the ACM, 43(7), pp. 125-128.

Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 04.05.2016, s. 1–88). Hämtad 17 juli 2019 från: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. Computers, Privacy & Data Protection, 14(3), 25.

Hoepman, J. H. (2014, June). Privacy design strategies. In IFIP International Information Security Conference (pp. 446-459). Springer, Berlin, Heidelberg.

Intention to fine British Airways £183.39m under GDPR for data breach. (2019, july 8a). Hämtad 13 juli 2019 från: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach. (2019, july 9b). Hämtad 13 juli 2019 från: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-GDPR-for-data-breach/

White House. (2011). National strategy for trusted identities in cyberspace.

Wylder J. (2003). Strategic Information Security, Auerbach Public