

En undersökning av förändringar som behöver införas för att överensstämna med GDPR

I utveckling och drift av smarta kameror

An investigation of changes that need to be introduced to comply with GDPR

In the development and operation of smart cameras

Andrea Lukacs & Malgorzata Szczurek

Informatik
Kandidatnivå
13 hp
VT2018

Handledare: Annabella Loconsole och Zahra Ghaffari

Abstract

The concept of the Internet of Things is about computers being able to act without human interaction. This allows smart alarms with cameras to determine themselves when an alarm is triggered and can take action like taking pictures at home that cameras are installed in as well as on individuals. This creates some ethical issues related to data privacy. In order to control companies' use of amounts of data that can be generated today and to give individuals rights over how their data is processed, the EU has developed a regulation called the General Data Protection Regulation (GDPR). This will change the development and operation of smart cameras, as images are personal data that are covered by the regulation. Therefore, clear strategies about the changes that needs to be implemented to meet the GDPR requirements is necessary to maintain users' data privacy. The purpose of the project is therefore to account for major changes that need to be introduced to companies identical to the study objects while taking into account the attitude towards the change, which is a key factor for successful implementation. This is achieved through data acquisition through interviews conducted by companies leading in the development and operation of smart cameras. The result confirms the hypothesis that camera and security companies are experts in security and integrity, as well as demonstrating that companies are dealing with five, the following major changes: finding solutions for collecting informed consent, documentation that needs to be more detailed, contracting with suppliers must be paid more attention to, make it technically possible for a customer to request and get all data, as well as Privacy by Design and an overall perspective that needs to be implemented during the development process. In addition, the work can be used as a basis for decision making in similar organizations as the study objects who develop IoT products, as it also provides suggestions for improvement areas that intend to enhance the possibility of a successful satisfaction of the GDPR requirements.

Key words

Internet of Things (IoT), General Data Protection Regulation (GDPR), Smart Alarm, Smart Cameras, Change, Security, Privacy

Sammanfattning

Konceptet av sakernas internet handlar om att datorer ska kunna agera utan mänsklig interaktion. Detta gör att smarta larm med kameror själva kan avgöra när ett larm ska utlösas och kan då ta åtgärder som att ta bilder på hemmet som kameror är installerade i samt på individer. Detta skapar vissa etiska frågor kopplade till dataintegriteten. För att kunna kontrollera företagens användning av mängder data som kan genereras idag och för att ge individer rättigheter över hur deras data behandlas har EU tagit fram en förordning kallad General Data Protection Regulation (GDPR). Denna kommer att förändra utveckling och drift av smarta kameror, eftersom bilder är personuppgifter som omfattas av förordningen. Därför är tydliga strategier kring vilka förändringar företag som utvecklar eller driftar kameror behöver införa för att uppfylla GDPR kraven nödvändiga för att upprätthålla användarnas dataintegritet. Projektets syfte är därför att redogöra för huvudsakliga förändringar som behöver införas hos företag identiska till studieobjekten samtidigt som inställningen till förändringen beaktas, vilket är en nyckelfaktor till en lyckad implementering. Detta uppnås genom datainsamling via intervjuer som utfördes hos företag ledande inom utveckling och drift av smarta kameror. Resultatet bekräftar hypotesen om att kamera och säkerhetsföretag är sakkunniga inom säkerhet och integritet, samt visar att företag handskas med fem, följande, huvudsakliga förändringar: finna lösningar på insamling av informerade samtycken, dokumentation som måste bli mer utförlig, kontraktskrivning med leverantörer måste ges mer uppmärksamhet, att möjliggöra framförallt i backenden när en kund begär ut all data, samt privacy by design och ett helhetsperspektiv som behöver implementeras mer under utvecklingsprocessen. Vidare kan arbetet användas som beslutsunderlag i liknande organisationer som studieobjekten, eftersom det ger även förslag på förbättringsområden vilka har för avsikt att förstärka möjligheten till en lyckad tillfredsställelse av GDPR kraven.

Nyckelord

Internet of things (IoT), General Data Protection Regulation (GDPR), smarta larm, smarta kameror, förändring, säkerhet, integritet

Acknowledgements

We would like to thank our supervisors Annabella and Zahra for the feedback and input, as well as Joseph Bugeja for letting us bounce ideas off him. Special thanks to everyone who agreed to do interviews with us. Without you we would not be able to collect data.

Innehållsförteckning

| | |
|---|----|
| 1. INTRODUKTION | 3 |
| 1.1 Tidigare forskning | 4 |
| 1.2 Problemformulering | 6 |
| 1.3 Studiens syfte | 7 |
| 1.4 Forskningsfråga | 7 |
| 1.5 Avgränsningar | 7 |
| 1.6 Begreppsdefinitioner | 8 |
| 2. METOD | 11 |
| 2.1 Forskningsstrategi | 11 |
| 2.2 Val av studieobjekt | 11 |
| 2.3 Datainsamlingsmetod | 12 |
| 2.4 Val av respondenter | 12 |
| 2.5 Genomförande och kodning av intervjuer | 13 |
| 2.6 Analysmetod | 15 |
| 2.7 Etiska riktlinjer | 16 |
| 2.8 Källkritik | 16 |
| 2.9 Triangulering | 17 |
| 3. TEORETISKT RAMVERK | 18 |
| 3.1 Informationssäkerhet och integritet | 18 |
| 3.2 Inställning till och motivation i förändringar | 18 |
| 3.3 Implementation av förändringar i samband med GDPR | 19 |
| 4. EMPIRI | 21 |
| 4.1 Informationssäkerhet och integritet före GDPR | 21 |
| 4.1.1 Dagens tillstånd | 21 |
| 4.1.2 Säkerhet | 22 |
| 4.1.3 Dataintegritet | 23 |
| 4.2 Anställdas inställning till och förståelse för GDPR | 24 |
| 4.2.1 Tydlighet | 24 |
| 4.2.2 Användbarhet | 24 |
| 4.2.3 Brister | 25 |
| 4.2.4 Begränsning eller möjlighet | 26 |
| 4.3 Implementation av förändringar i samband med GDPR | 26 |
| 4.3.1 Utmaningar | 26 |
| 4.3.2 Kommunikation och samarbete mellan avdelningar | 28 |
| 4.3.3 Vilka arbetar med GDPR och hur? | 28 |

| | |
|---|----|
| 4.3.4 Vilka förändringar behöver göras? | 29 |
| 4.3.5 Implementering och uppföljning | 29 |
| 5. ANALYS | 31 |
| 5.1 Informationssäkerhet och integritet före GDPR..... | 31 |
| 5.2 Anställdas inställning till och förståelse för GDPR | 32 |
| 5.3 Implementation av förändringar i samband med GDPR..... | 34 |
| 6. DISKUSSION..... | 37 |
| 6.1 Informationssäkerhet och integritet före GDPR..... | 37 |
| 6.2 Anställdas inställning till och förståelse för GDPR | 38 |
| 6.3 Implementation av förändringar i samband med GDPR..... | 39 |
| 7. SLUTSATS..... | 41 |
| 8. FORTSATT FORSKNING | 43 |
| 9. REFERENSER | 44 |
| 10. BILAGOR..... | 1 |
| Bilaga 1 - Information om studiens syfte skickat till respondenter..... | 1 |
| Bilaga 2 - Samtyckesblankett för intervjuer..... | 2 |
| Bilaga 3 - Frågor till intervjuer | 5 |

1. INTRODUKTION

I detta kapitel presenteras bakgrunden till studien och frågeställningen. Under 1.6 behandlas definitioner av begrepp som är relevanta både för att tydliggöra tolkningen av dessa och samtidigt för att ge läsaren en tydlig förståelse inför resterande delen av studien.

Internet of Things översätts på svenska till "sakernas internet" och beskriver ett system med enheter som innehåller inbyggda elektroniska delar. Dessa delar gör det möjligt att koppla upp enheterna tillsammans och få dem att interagera med varandra utan människors ingripande. Med hjälp av internet kan interaktionen ske på distans och utan en fysisk uppkoppling. (Rouse, 2016)

Tekniken används bland annat i utvecklingen av så kallade smarta larm. Dessa larm installeras med smarta kameror, som samlar information i bildform (och i vissa fall även i ljudform) från användarnas egna hem vid utlösning av ett larm och kan skicka bilderna till en larmcentral.

Mängden av IoT apparater växer ständigt (Bugeja, Jacobsson och Davidsson, 2017) vilket kommer att innebära en ökning med 20 miljard anordningar mellan åren 2015 och 2020 (Gartner, 2015). Intresset har växt tillsammans med investeringar i företag som skulle utveckla produkter relaterade till IoT (PCWorld from IDG, 2016). Den uppskattade ökningen av IoT tillbehör påvisar teknikens popularitet och framtida existens.

Konceptet med datorer som finns överallt och i olika former har i litteraturen beskrivits med flera namn. Nieuwdorp (2007) använde det engelska ordet Pervasive, medan Kevin Ashton myntade begreppet Internet of Things (som förkortas IoT) år 1999 (Ashton, 2009). Det som Kevin Ashton menade (Ashton, 2009) var att i dåvarande läge var datorer (och därför även internet) väldigt beroende av människor. Nästan all data tillgänglig på nätet hade genererats av människor genom att exempelvis skriva på tangentbordet eller ta foton. Utmaningen var att människor har begränsad tid, uppmärksamhet och noggrannhet, vilket gör att de är bristfälliga när det kommer till att samla data om den riktiga världen. IoT erbjuder då möjligheten att samla in obegränsade mängder data, speciellt olika typer av data från sensorer utan användarens fullständiga medvetenhet (Niese et al, 2016).

Utöver det är området IoT redan komplext. *"I teorin är det önskvärt att så mycket som möjligt av data som samlas av en IoT enhet görs tillgängligt för andra enheter. Sätt som detta kan åstadkommas på är oräkneliga. Det är således viktigt att studera behovet av och utformningen av mekanismer för integritetsskydd för att säkerställa användarnas integritet."* (Internet of Things and People, u.å.)

Avsikten och användandet av den insamlade datan kan vara diskrepant (Jacobsson, Boldt och Carlsson, 2015), vilket innebär att avsikten med att kameran tar en bild på hemmet kan vara för att upptäcka en eventuell brand, men om samma bild ses av en obehörig kan den exempelvis användas till att bryta sig in i hemmet. En annan konsekvens kan vara att inspelningar från kameror i en persons hem modifieras med hjälp av s.k. facial reenactment vilket är en teknik som har använts i filmindustrin men har utvecklats till att modifiera existerande videoinspelningar i realtid (Thies et al., 2016) med avsikt att förstöra personens rykte eller sprida falsk information om vad personen har sagt. Niclas Kjellin (2018) menar att läckta personuppgifter även kan användas till bland annat bedrägerier och utpressning. Mer än 9 miljarder personuppgifter har enligt Kjellin (2018) läckt sedan 2013. Därför är den

sortens data särskilt känslig ur en integritetssynpunkt som Bugeja et al. (2017) förklarar genom: *“A home is the place where privacy is expected to be respected”*.

Bugeja, Jacobsson och Davidsson (2017) menar att användarna har ett intresse kring att ha sin personliga data skyddad. Samtidigt menar Bugeja et al. (2017) att tidigare forskning fokuserar främst på nätbaserade system och inte på IoT apparaters sårbarhet. Bugeja et al (2018) undersökning om sårbarheter visade att osäker konfigurationshantering och otillräcklig autentisering var orsakerna till smarta kamerors sårbarhet när det gäller tillgänglighet på Internet. Författaren kom fram till att det fanns flera hundra tusen smarta kameror på nätet med data tillgänglig för vem som helst.

Om integriteten av användarnas data som smarta kameror samlar in inte är skyddad av företag kan informationen utnyttjas av obehöriga. Obehörig tillgång och missbruk av datan kan enligt Sherwood et al (2005, 14) påverka förtroendet för produkten och även för företaget. Avsaknad av förtroendet kan leda till minskat engagemang från användare för att nyttja produkten. Minskat engagemang kan till och med resultera i att företag förlorar kunden. Enligt Sommerville (2011) avvisar användare ofta system som är opålitliga eller osäkra, vilket bekräftas av statistik (Svenskarnas syn på IT-säkerhet 2017), enligt vilken 96% skulle sluta samarbeta med en organisation som har läckt eller missbrukat personuppgifter. Därför finns det ett behov för strategier som stödjer kundernas förtroende från en säkerhetssynpunkt, utan vilka marknadsandelar eller viktiga samarbetspartners kan gå förlorade (Internet of things and people, u.å., Sentor, 2018).

Av dessa orsaker är förtroendet för smarta kameror en nyckelfaktor. Jacobsson et al. (2015) menar därför att företagens transparens mot användarna om hur deras data behandlas, analyseras och används är en grundläggande förutsättning.

För att säkerställa transparens i hur data används har det tagits fram ett nytt regelverk som ska gälla i alla EU:s medlemsländer och dess medborgare. Den benämns dataskyddsförordningen (GDPR) och träder i kraft i maj 2018. GDPR enligt Kjellin (2018) kan beskrivas som: *“Common sense for personal data protection”*. Dataskyddsförordningen kommer att medföra förändringar kring behandling av personuppgifter och härda rättigheter för personlig integritet (Datainspektionen, 2018). GDPR skapar en enhetlig lag för hela EU och har en bred definition av personlig data: *“varje upplysning som avser en identifierad eller identifierbar fysisk person”* (Datainspektionen, 2018) och reglerar användning av datan. Digitala identifierare, fotografier och data skapad av IoT räknas också som personuppgifter (Kjellin, 2018), vilket betyder att datan från smarta kameror innefattas av förordningen. Samtidigt menar Kjellin (2018) att det är användarna som får rättigheter och företagen som har ansvaret. Vidare tillägger han att det innebär ett slags problem för de som är utvecklare för ett system. Straffen för att inte följa lagen är mycket strikt, i form av 2-4% av omsättningen.

1.1 Tidigare forskning

Tidigare forskning finns inom området av säkerhet och dataintegritet inom det smarta hemmet (Bugeja et al, 2017; Bugeja et al, 2018; Jacobsson, 2016) och inom utmaningar med GDPR (Junwoo et al, 2017; Lindqvist, 2017; Tankard, 2016), men hur GDPR förändrar företagens förhållningssätt till dataintegritet i processen från utvecklingen av kameror till deras drift behandlas inte, vilket därför är en kunskapslucka. Svaret på dessa frågor kommer därför att generera ny kunskap om hur IoT företag som utvecklar eller driftar smarta kameror planerar och anpassar utvecklingen av sina produkter genom hela värdekedjan efter

att GDPR regelverket träder i kraft. Nedan presenteras relaterad forskning inom informatikområdet som är adekvat till studien:

Säkerhetsbrister med smarta kameror som påverkar integritet

Bugeja, Jönsson och Jacobssons (2018) studie visar att smarta kameror har flera säkerhetsbrister som påverkar integriteten genom att exempelvis obehöriga med hjälp av sökmotorn Shodan får tillgång till de smarta kamerornas bild. Målet med deras experiment var att påvisa allvaret i situationen och föreslå eventuella lösningar. Bugeja et al (2018) analyserade datan från 542 270 kameror utifrån sårbarheter och sammanställde en riskanalys utifrån allvarlighet. Just den smarta kameran (Axis 2100, CVE-2007-5213) i hemmet fick kategoriseringen "hög" risk, eftersom obehöriga kan komma över fullständigt privilegium till kamerans data. Just bilder och video som kameran spelar in är speciellt känsliga ur en integritetssynpunkt. Intressant att Bugeja et al (2018) menar att det bara krävdes tillgång till internet och sökmotorn Shodan för att samla in all data från mängder av smarta kameror. En intressant upptäckt av Bugeja et al (2018) är att det finns smarta uppkopplade kameror som inte har inbyggd automatisk uppdatering. Bugeja et al (2018) rekommenderar därför företag att utföra riskbedömningar under utvecklingsarbetet av smarta kameror. Bugeja et al (2018) förstärker studiens argument om att företag behöver tydliga strategier för att skydda användarnas integritet, eftersom det är relativt enkelt för en bedragare att komma åt en kameran data. Bugeja et al (2018) överlämnar en rekommendation, denna studie kommer att framföra huvudsakliga förändringar som företag behöver implementera för att överensstamma med GDPR-kraven.

GDPR innebär ekonomiska utmaningar för företag

Junwoo, Kyoungmin, Mookyu, Moosung och Kyungho (2017) bevisar att GDPR även innebär ekonomiska utmaningar för IoT företag. Författarna undersöker den ekonomiska inverkan i följd av förordningen hos IoT näringslivet och konstaterar att efter dataskyddsförordningen träder i kraft kan företagens kostnader tre- eller fyrdubblas. Junwoo et al (2017) har använt Gordon & Loeb's modell för att beräkna kostnadsökningen. I artikeln analyseras fyra fall av dataförlust och beräknas först kostnaderna för IoT företag innan GDPR, samt möjliga kostnader efter dataskyddsförordningen träder i kraft. Junwoo et al (2017) slutsats är att GDPR och dess inverkan ökar spänningen hos företag, vilket underbyggs med statistik som visar att: 52% av företagen är oroliga över att förordningen kommer innebära böter, 65% av företagen funderar på att byta sina affärsstrategier och 30% tror att GDPR kommer att föröka deras årliga budget med mer än 10% tills förordningen blir implementerad. Junwoo et al (2017) undersökningsresultat påvisar kostnadsökningen och oroligheten hos IoT företag i följd av dataskyddsförordningen. Just spänning och orolighet kan ha en negativ påverkan på engagemang hos anställda under en förändring, vilket förstärker tanken om att anställdas inställning till förändring är nödvändigt att beakta vid implementering av GDPR-kraven. Junwoo et al (2017) studie används som ett underlag till att påvisa både spänningen hos företag i IoT branschen och allvarligheten av konsekvenser som förordningen för med sig i form av böter. Junwoo et al (2017) fokuserar på kostnadsökning, denna studie fokuserar på organisatoriska förändringar i följd av GDPRs implementering.

Problematiskt att implementera Artikel 28 i en IoT kontext

Lindqvist (2017) undersöker om GDPR passar för att hantera teknologier som IoT och lägger fokus på att kartlägga relationsförändringar bland IoT intressenter i följd av GDPR. Hans mål var att utforska om dataskyddsförordningen är lämplig för IoT apparater, eftersom relationen mellan "databehandlare" och "datakontrollant" (vilka definieras mer utförligt i studien)

företag har blivit allt mer komplicerad på grund av den snabba teknologiska utvecklingen. Lindquist (2017) menar att olika aktörer delar ansvaret över dataprocess och datakontroll vid IoT, eftersom olika intressenter är involverade i själva IoT processen. Enligt författaren är Artikel 28 i GDPR, som handlar om kontrakt mellan intressenter problematiskt att implementera i en IoT kontext. Dataskyddsförordningen är därför inte anpassat till alla nya teknologier, bland annat IoT, vilket kan leda till förvirring och osäkerhet bland företag som behöver tillämpa förordningen, vilket alla organisationer som riktar sig till kunder inom EU behöver göra. Artikeln fokuserar på legala kontrakt mellan intressenter inom IoT och dess utmaningar, fokuset i denna uppsats kommer ligga på att undersöka huvudsakliga förändringar och förbättringsmöjligheter i utveckling och drift av smarta kameror.

GDPR - tydliga strategier är nödvändiga

I och med att GDPR träder i kraft i maj 2018, kommer alla företag som hanterar personlig information påverkas av förordningen. Därför kommer alla företag enligt Tankard (2016) behöva implementera tydliga strategier, rutiner och processer för att uppnå kravet. Tankard (2016) föreslår en generell "best practice framework" till organisationer med målet att erbjuda en mall för att uppnå större effektivitet och hållbarhet i operationer. Tankards (2016) mall har ett holistisk perspektiv, och innehåller inga konkreta förslag till just en utvecklingsprocess av smarta kameror. Det kan därför vara intressant att undersöka hur företag som utvecklar och drifvar smarta kameror arbetar med utvecklingsprocess och drift av smarta kameror för att säkerställa att bilder från kameror inte skulle kunna bli kopplade till en specifik individ. Tankards (2016) studie används som ett underlag till vårt förhållningssätt om att tydliga strategier, rutiner och processer är nödvändiga för företag till att uppfylla GDPR-kraven. Tankard (2016) undersöker dock inte just företag som utvecklar eller drifvar smarta kameror och beaktar inte heller just IoT branschens utmaningar och bildernas känslighet ur integritetssynpunkt vilket denna studie har för syfte att uppnå.

Säkerhetsbrister med smarta kameror

Zerlang (2017) beskriver i sin artikel att Internet of Things apparater hackas genomsnittligt inom 360 sekunder efter att dessa går online och härmed blir som baddörrar i annars säkra nätverk. Därför menar Zerlang (2017) att säkerhetslösningar måste vara allomfattande, för att varenda element kan vara utsatt för hot. Colesky et al (2016) menar att mjukvara som är designad utifrån GDPR förordningen från början resulterar i mindre juridiskt arbete senare.

1.2 Problemformulering

Området är komplext. Det finns säkerhetsbrister med smarta kameror som påverkar individens integritet. Elovsson (2018) GDPR-ansvarig på Sentor menar att företag inte kan fullständigt skydda sig från dataläckor eftersom det kan finnas flera säkerhetsrelaterade kryphål i systemen vilka kan missbrukas av obehöriga, vilket innebär att det finns utrymme till förbättringar. GDPR måste följas av alla företag oavsett om det är svårt att implementera. Tydliga strategier kring vilka förändringar som företag inom IoT branschen behöver åstadkomma för att uppfylla GDPR-kraven är nödvändiga för att upprätthålla dataintegritet. För att kunna göra detta måste dock förändringar som behöver implementeras identifieras. Enligt Foster (2010) förenklar engagemang och uppslutning bland medarbetare en organisatorisk förändring i motsats till motstånd som försvårar den, vilket innebär att anställdas inställning till förändringen och drivkrafter även måste undersökas och beaktas.

1.3 Studiens syfte

Temat som undersöks i arbetet är därför hur företag som utvecklar och erbjuder drift av smarta kameror anpassar sig till den nya lagstiftningen för att kunna förstå vilka förändringar som behöver utföras och därefter kunna skapa strategier utifrån dessa. Eftersom området är väldigt stort läggs fokus endast på smarta kameror som är tänkta att ta bilder på hemmet vid en eventuell utlösning av larmet. Smarta kameror valdes, eftersom just bilder betraktas som väldigt känsliga ur integritetssynpunkt.

Syftet med studien är att hitta och presentera huvudsakliga förhållanden som behöver förändras i utveckling och drift av smarta kameror. Resultatet ska vara användbart för studiens målgrupp som är företag av den typen som arbetet undersöker. Studien presenterar även förslag på förbättringsområden för studieobjekten.

1.4 Forskningsfråga

Hypotesen är att företag som är involverade i utveckling och drift av smarta kameror redan uppfyller GDPR-kraven bättre än företag i andra branscher, eftersom just säkerhet är deras kärnprodukt. Trots det kan enligt tidigare forskning finnas utrymme till förbättring av företagens dataintegritets-mekanismer. Teorier visar även på att för en lyckad implementering av förändringar är anställdas inställning en nyckelfaktor. Det är därför relevant att vid beforskning av förändringar även undersöka anställdas inställning och dess påverkan på utfallet av förändring, vilket motiverar valet av delfråga 2. Det är även nödvändigt att undersöka omständigheten innan förändringen för att dels bekräfta hypotesen och samtidigt uppnå en tydlig förståelse för vilka områden förändringen påverkar. Forskningsfrågan som ställs är därför: *“Vilka förändringar behöver företag implementera för att uppfylla GDPR-kraven jämfört med tillståndet innan samt vilken inställning har anställda till förändringen i utveckling och drift av smarta kameror för att implementeringen skall bli lyckad?”*

Forskningsfrågan bryts upp i följande delfrågor för att dels maximera upptäckten inom alla områden som forskningsfrågan behandlar och samtidigt för att visa på en tydlig koppling bland områdena under studien:

- 1. Hur ser företagens tillstånd och arbete med säkerhet och dataintegritet ut före GDPR vid utveckling och drift av smarta kameror?*
- 2. Vilken inställning och förståelse anställda har till GDPR vid utveckling och drift av smarta kameror?*
- 3. Vilka förändringar kommer företag behöva implementera för att uppnå GDPR-kraven vid utveckling och drift av smarta kameror?*

Tillståndet innan förändringen, det vill säga nuläget undersöks av forskningsfråga 1 och behandlas i 3.1, 4.1, 5.1, samt 6.1. Inställning och engagemang, alltså anställdas förståelse av och attityd mot GDPR undersöks av forskningsfråga 2 och behandlas i 3.2, 4.2, 5.2, samt 6.2. Planerade förändringar som implementeras undersöks av forskningsfråga 3 och behandlas i 3.3, 4.3, 5.3, samt 6.3.

1.5 Avgränsningar

Arbetet innefattar inte tekniska detaljer om smarta kameror och IoT lösningar, eftersom det inte är nödvändigt för att besvara forskningsfrågan. Tekniska detaljer faller därför utanför

undersökningens gräns. Mjukvarusystem är inte isolerade system utan snarare väsentliga komponenter av mer omfattande system som har något mänskligt, socialt eller organisatoriskt syfte (Sommerville, 2011). Integritet skapas under både utveckling och drift av en smart kamera. Därför undersöks endast hur dataintegritet säkerställs genom hela kedjan från utvecklingen av mjukvaran i kameror till uppkopplingen till resten av larmsystemet. Avgränsningen görs till datasäkerhet och integritetsaspekter av GDPR. I arbetet nämns ISO 27001, vilket förklaras övergripande, men att studera det noggrant ansågs ligga utanför studiens ramar. En avgränsning gjordes även till att undersöka GDPR:s påverkan på förändringar endast inom EU.

1.6 Begreppsdefinitioner

Smarta larm

Belbachir (2010) skriver att Automated imaging association (AIA) definierar tre väsentliga funktioner för att kameror ska klassificeras som smarta. 1. Integrering av vissa nyckelfunktioner i enheten (t.ex. optik, belysning, bildåtergivning och bildbehandling). 2. Användning av en processor och programvara för att uppnå beräkning på någon nivå. 3. Förmågan att utföra flera uppgifter utan att kräva manuella åtgärder. Ett exempel kan vara när en kamera övervakar en dörr och utlöser ett larm när någon försöker ta sig in efter stängningstid. Denna skulle kvalificeras som en smart kamera, eftersom den kan ta reda på vad som händer och vidta åtgärder.

Det finns dock andra inbyggda visionsystem som också kan klassificeras som smarta kameror trots att de inte verkar vara fristående kameror. Många av dessa system kallas faktiskt smarta kameror inom akademien och i forskningslitteratur. Visionssystem är datorbaserade enheter eller system, där hårdvaran (t.ex. sensorer, processorer, datorer, nätverk) och programvaran (t.ex. datoralgoritmer) arbetar tillsammans för att utföra uppgifter som liknar mänsklig syn. Det som är gemensamt för både smarta kameror och visionssystem är att de själva kan, utan mänskliga åtgärder ta bilder när det behövs. Av denna anledning behandlas båda i detta arbete men kallas för enkelhetens skull smarta kameror eller smarta larm.

Säkerhet

Sommerville (2011) definierar säkerhet som systemets förmåga att skydda sig mot oavsiktlig eller avsiktlig intrång, Carroll et al (2012) beskriver säkerhet som en gräns mellan drift av maskiner och användarnas beteende. Säkerhet används för att skydda värdefulla tillgångar i affärsmiljön. Om dessa tillgångar skadas eller förloras, kommer det att innebära en negativ inverkan på affärsverksamheten.

Informationssäkerhet

Sherwood et al (2005, 5) beskriver informationssäkerheten som en affärsmöjliggörare (business enabler). Avslöjandet av personlig information är en stor affärsrisk. Tillgångarna försvaras då med ett skyddslager genom säkerhetskontroller, för att hålla hoten borta från verksamhetens tillgångar. (Sherwood et al, 2005, 4)

Dataintegritet

Enligt Sommerville (2011) betyder dataintegritet: personal data konfidentialitet, vilket IT Governance Privacy Team (2016) uttrycker som att personal information görs ej tillgänglig till obehöriga individer, enheter eller processer.

GDPR

Dataskyddsförordningen (GDPR) träder i kraft i maj 2018 och kommer att gälla i alla EUs medlemsländer. GDPR har följande 6 principer. Datan ska: 1. bearbetas lagligt, rättvist och på ett öppet sätt, 2. samlas för specifika, explicita och legitima syften, 3. vara relevant och begränsad till vad som är nödvändigt, 4. vara noggrann och vid behov hållas uppdaterad, 5. behållas endast så länge som nödvändigt, 6. bearbetas på ett lämpligt sätt för att upprätthålla säkerheten. Lagen innebär även att 1. personen vars data bearbetas måste ha gett en tydlig, frivillig tillåtelse, 2. personen ska ha möjlighet att ändra på och ta bort datan om så önskas, 3. det ska gå att använda tjänsten utan att godkänna databehandling, 4. organisationen måste definiera vem som har tillgång till datan och hålla koll på var den är sparad, 5. om det sker en läcka av datan måste organisationen inom 72 timmar informera om detta och berätta vems data som har påverkats (Damore, 2017).

Privacy by design

Privacy by design enligt IT Governance Privacy Team (2016) är en process som har sekretess som utgångspunkt och säkerställer det genom all persondata insamling, bearbetning, lagring och förstörelse.

Agila metoder vid utveckling

Agila metoder bygger allmänt på ett inkrementellt tillvägagångssätt för programvaruspecifikation, utveckling och leverans. Enligt Sun och Schmidt (2018) genom involvering av kunder, fokus på människor istället för process och upprätthålla enkelhet. Metoden är bäst lämpad för applikationsutveckling där systemkraven vanligtvis förändras snabbt under utvecklingsprocessen. De är avsedda att snabbt leverera fungerande program till kunder, som sedan kan föreslå nya och ändrade krav som ingår i senare iterationer av systemet (Sun och Schmidt, 2018).

Kravspecifikationer

Sommerville (2011) pratar om att i kravspecifikationer delas krav ofta upp i funktionella och icke funktionella. Funktionella beskriver vad systemet borde göra och beror på vilken typ av programvara som utvecklas, dess användare och det allmänna tillvägagångssättet som organisationen tar när man skriver krav. Icke-funktionella krav, som namnet antyder, är krav som inte är direkt berörda av de specifika tjänster som systemet levererar till sina användare. De kan relatera till framväxande systemegenskaper som tillförlitlighet, svarstid och beläggning. Alternativt kan de definiera begränsningar på systemimplementeringen. Icke-funktionella krav, såsom prestanda, säkerhet eller tillgänglighet, brukar ange eller begränsa egenskaper hos systemet som helhet. Icke-funktionella krav är ofta mer avgörande än enskilda funktionella krav. Systemanvändare kan vanligtvis hitta sätt att arbeta runt en systemfunktion som inte riktigt uppfyller deras behov. Att inte uppfylla ett icke-funktionellt krav kan dock innebära att hela systemet är oanvändbart. Ett enda icke-funktionellt krav, såsom ett säkerhetskrav, kan generera ett antal relaterade funktionskrav som definierar nya systemtjänster som krävs. Dessutom kan det också skapa krav som begränsar befintliga krav.

Enligt Sommerville (2011) är programvarukravsspecifikationen ett officiellt uttalande om vad systemutvecklarna ska genomföra. Det ska innehålla både användarkraven för ett system och en detaljerad specifikation av systemkraven. Ibland integreras användar- och systemkraven i en enda beskrivning. I andra fall definieras användarkraven i en introduktion till kravspecifikationen. Om det finns ett stort antal krav kan detaljerade systemkrav presenteras i ett separat dokument.

Organisationsförändring

Enligt Jacobsen och Thorsvik (2008, 39) framställer strategin tillvägagångssättet mot ett mål, vilket enligt författaren är en önskad framtida position. Vidare hävdar Jacobsen och Thorsvik (2008, 414) att förändringar kan handla exempelvis om processförändringar, strategibyte, kulturförändringar och måljustering i en organisation. Om en förändring äger rum eftersom något inträffar i omvärlden, då kallas det för en proaktiv förändring (Jacobsen och Thorsvik, 2008, 416).

ISO 27000

ISO 27001 står för international standard organisation och är en internationell, ackrediterad external certifiering för ett ledningssystem för informationssäkerhet förvaltning. Syftet med ISO 27001 är att skydda konfidentialitet, integritet och tillgänglighet av information genom att applicera en risk management process vilket erbjuder förtroende för att riskerna hanteras på ett korrekt sätt (IT Governance Team, 2016).

Uppmuntrande ledarstil

Enligt Yukl (1999) kan ledarens syn på arbetare påverka deras motivation. När ledaren utgår från att anställda har förmågan och förväntar sig att de kommer göra ett tillfredsställande jobb presterar anställda bättre, jämfört med en negativ syn när ledaren anser att anställda inte kan eller vill. Ledarstilen fokuserar därför på stödja och tro på den enskilda individen i syfte att motivera.

2. METOD

I följande kapitel beskrivs strategin och tillvägagångssättet för genomförandet av studien. Val av studieobjekt och respondenter presenteras och det redogörs för etiska riktlinjer och källkritik. De gjorda valen angående metod diskuteras och motiveras i detta kapitel.

2.1 Forskningsstrategi

Utgångspunkten var att förhålla sig till ett kvalitativt perspektiv, vilket enligt Backman (2016) innebär ett subjektivt synsätt i motsatsen till det traditionella synsättet som är relativt objektivt. I det tidiga skedet var forskningsfrågan oklar och forskningen skulle därför delvis vara av utforskande typ, därför valdes det kvalitativa synsättet. Kvalitativ forskning ger till skillnad från kvantitativ möjligheten att gå på djupet. Avsikten var att uppnå detta för att belysa intressanta aspekter och inte hitta mönster. Därför valdes kvantitativ forskningsstrategi bort och forskningsgruppen bestämde sig för att förhålla sig till en kvalitativ ansats.

Vid val av metod diskuterades olika av kvalitativ typ, som skulle kunna användas för studien. Forskarna var inte involverade i företagets genomförande av förändringar och företagen var inte involverade i forskningens utformning, vilket gjorde att aktionsforskning inte var en passande metod för studien. Forskningen skulle inte heller bidra med artefakter, därför valdes design-baserad forskning bort. Fältdarbete med observationer och detaljerade beskrivningar ansågs inte lämpliga för att besvara forskningsfrågan, eftersom studien syftade till att undersöka avsiktliga förändringar inte utfallet, vilket gjorde att etnografiska studier även valdes bort. Enligt Denzin och Linkoln (2005) kopplar strategier forskaren till specifika metoder av insamling och analys av empiriskt material men de behöver inte hanteras som specifika tillvägagångssätt, som måste följas. Trots allt är flexibilitet en av styrkorna med kvalitativ forskning, vilket enligt Denzin och Linkoln (2005) innebär att forskaren kan sätta samman metoder eller använda delar av dessa specifikt till det egna arbetets syfte.

Fallstudie som forskningsstrategi ansågs mest passande, eftersom den möjliggör enligt Denscombe (2016) att undersöka förhållanden och processer. Dess syfte är att belysa allmängiltighet genom att granska en specifik händelse, vilket sammanfaller med uppsatsens syfte som är att sammanställa ett resultat som är användbart för andra företag av den typen som undersöks. Dessutom ger fallstudie som strategi möjlighet till att undersöka relationer mellan specifika studieobjekt för att förstå varför händelser inträffar, vilket ansågs som relevant för att uppnå syftet. Fallstudie ger även möjlighet till ett holistiskt perspektiv, vilket enligt Denscombe (2016) erbjuder möjlighet till att upptäcka hur olika delar som exempelvis avdelningar påverkar varandra, vilket även stämmer överens med syftet. Denscombe (2016) nämner trovärdigheten i generaliseringar som görs i en fallstudie som kan vara känsliga för kritik med fallstudier, därför bestämdes ett kritiskt förhållningssätt till det egna arbetet när det gäller generaliseringar. Vidare nämner Denscombe (2016) att det kan vara problematiskt att definiera fallets gränser på ett tydligt sätt när forskaren bestämmer sig över datakällor. Fallets gränser, samt källor som beaktas i undersökningen beskrivs och presenteras därför tydligt: medvetet fokuserar forskningen endast på GDPR:s påverkan på de utvalda studieobjektens utveckling och drift av smarta kameror, andra kontextuella faktorer beaktas inte på grund av att dessa faller utanför fallets gränser samt är inte nödvändiga till att besvara forskningsfrågan.

2.2 Val av studieobjekt

Vid val av studieobjekt gjordes ett antagande om att företag som erbjuder tjänster inom säkerhet och övervakning bör vara mer framstående inom just säkerhet och dataintegritet än

företag inom andra branscher på grund av erfarenheten från det dagliga arbetet, samt behovet att skapa en enhetlig bild av ett pålitligt system. Vid insamling av empirisk data undersöktes företag som tillverkar kameror och kunde erbjuda information om vilka säkerhetslösningar som finns idag för att förhindra att obehöriga kommer åt data i deras produkter, företagets inställning till GDPR och utmaningar till förändring. Följande studieobjekt stämde överens med dessa krav: ett företag som utvecklar smarta kameror, ett ledande företag inom försäljning av smarta larm som kunde erbjuda information om vilka strategier de har för att förhindra kryphål i hela det smarta larm systemet, samt ett företag som både utvecklar och försäljer smarta larm. Detta, eftersom det skulle täcka hela kedjan från produktion till uppkoppling, vilket är studiens fall. Företagens identitet avslöjas ej. Orsaken till det är ämnets känslighet. För att få in andra perspektiv intervjuas även två experter inom säkerhetsområdet.

I syfte att kunna få djupare förståelse om hur företag generellt kan säkerställa användarnas integritet undersöktes studieobjektens strategi under utveckling för drift av smarta kameror.

2.3 Datainsamlingsmetod

Intervjuer som datainsamlingsmetod valdes, för att samla in värdefulla insikter och undersöka forskningsområdet djupgående, vilket enligt Denscombe (2016) finns bland fördelarna med intervjuer. Nackdelar som datans validitet och intervjuareffekten beaktas under tolkningen och analysen av materialet. Intervjuareffekten innebär enligt Denscombe (2016) att respondenterna kan ge olika svar beroende på hur de själva uppfattar forskaren. Därför var forskarna lyhörda och neutrala under genomförandet av intervjuer, för att maximera ärliga och utförliga svar.

Intervjuer genomfördes även med experter inom säkerhet, IoT och GDPR med målet att få en bred och djup förståelse. Det möjliggör även triangulering av den insamlade datan. Intervjuerna var semi-strukturerade, eftersom det enligt Denscombe (2016) ger möjlighet till att samla in mer utvecklade svar än med strukturerade intervjuer genom följdfrågor. Samtidigt gav semi-strukturerade intervjuer möjligheten att vägleda respondenterna i vad de ska berätta om för att få svar på alla tre delfrågor. Detta är nödvändigt för att kunna besvara forskningsfrågan. Vid strukturerade intervjuer hade det inte funnits möjlighet till fördjupning inom intressanta områden och vid ostrukturerade hade det inte funnits ordning på intervjuens förlopp.

Alla intervjuer genomfördes tätt inpå varandra, under två veckor i slutet av mars och början på april. Detta innebär att det är troligt att det sedan dess har skett förändringar, eftersom GDPR träder i kraft först den 25 maj, vilket faller samman med uppsatsens inlämningsdatum.

Data om användarnas synvinkel samlas in sekundärt, genom föregående års statistik: *Svenskarnas syn på IT-säkerhet* gjord i 2017 av företaget Sentor vilket användes till att bekräfta studiens relevans och nödvändighet.

2.4 Val av respondenter

Samtliga respondenter valdes på grund av deras arbete inom säkerhet och/eller anknytning till säkerhetsbranschen för smarta larm, vilket innebär att varenda respondent har hög förståelse för smarta larm och/eller GDPR antingen organisatoriskt, tekniskt eller innehar specialistkunskap inom området. Vissa respondenter har förståelse eller erfarenhet inom flera av områdena. Fördelen med detta är att respondenterna gav värdefulla insikter till att kunna besvara forskningsfrågan, men nackdelen är avsaknaden av vanliga anställdas åsikter, som kanske inte har samma upplevelser och förståelse av förändringarnas orsak och behov. En

annan nackdel med respondenterna kan vara att de försöker att inte få sina företag att framstå i dålig dager och ger därför en alltför positiv bild av verkligheten.

Transkriberingen av intervjuer uppvisas inte i rapporten, därför presenteras information om respondenter som är relevant för studien.

- *Respondent 1:* Arbetar i över sju år som säkerhets- och hårdvaruarkitekt, på ett företag som bl. a. utvecklar kameror agilt, på en gemensam mjukvaruplattform.
- *Respondent 2:* Arbetar sedan 2005 som mjukvaruchef på R&D, på ett företag som bl.a. utvecklar mjukvara till och installerar smarta larm. Företaget jobbar i projekt i 1 till 2 år. 95% av utvecklingen är teknisk med att styra kretsar, osv. Kameran är en liten del av systemet med sensorer och dylikt.
- *Respondent 3:* Arbetar sedan två månader tillbaka som informationssäkerhetschef, på ett företag som bl.a. i projekt utvecklar mjukvara till och installerar smarta larm. Arbetar för samma företag som Respondent 2.
- *Respondent 4:* Arbetar sedan tio år tillbaka som projektledare, på ett företag som bl.a. erbjuder säkerhetslösningar och larm som själva avgör vilka objekt är en människa och skickar då bilder till larmcentralen för mänsklig kontroll.
- *Respondent 5:* Doktorand som undervisar i informationssäkerhet, samt forskar inom integritet. Har tidigare arbetat som huvudchef för informationssäkerhet.
- *Respondent 6:* Arbetar med säkerhet och GDPR som konsult och har utvecklingsbakgrund.

2.5 Genomförande och kodning av intervjuer

Sammanlagt genomfördes sex intervjuer. Motiveringen till antalet intervjuer är McCrackens (1988) påstående om att kvalitativa studiernas syfte inte är att generalisera resultatet och därför förespråkar han ett noggrant urval av respondenter och en omsorgsfull förberedelse och arbete istället för en ytlig undersökning av många respondenter. McCrackens (1988) förklaring påverkade beslutet gällande antalet intervjuer.

Intervjuerna utfördes i följande steg:

1. Sammanställning av intervjumall och frågor
2. Planering och genomförande av intervjuer
3. Transkribering av intervjuer
4. Sammanställning av kategoriseringsmall
5. Kodning av intervjuer utifrån kategoriseringsmall
6. Kodning av intervjumaterial baklänges
7. Sammanställning och presentation av resultatet från intervjuer i flytande text
8. Validering av resultatet med respondenterna
9. Uppdatering av resultatet utifrån validering

Steg 1.

Följande mall användes vid sammanställning av intervjufrågor som är byggda utifrån delfrågorna. Kategori 1, 2 och 3 kommer att besvara vår delfråga 1. Kategori 4 kommer att ge svar på delfråga 2. Kategori 5 kommer besvara delfråga 3. Kategori 6 används till baklängesforskning (Wästerfors, 2008) för att bredda perspektivet och för att inte gå miste om intressanta upptäckter.

Tabell 1. Intervjumall

| Kategori | Underkategorier | Vad eftersöks |
|---|---|--|
| 1 Databehandling (Forskningsfråga 1) | 1. Generell beskrivning av processen (roller, avdelningar, rutiner) 2. Utmaningar 3. Uppdateringar 4. Datans livscykel och vilken data de har 5. Förvaring | Kommunikation, samarbete mellan avdelningar, tydlig strategi |
| 2 Dataintegritet (Forskningsfråga 1) | 1. Krav 2. Lösningar, kryptering | Deras lösningar och krav |
| 3 Säkerhet (Forskningsfråga 1) | 1. Krav 2. Lösningar (exempelvis kryptering) 3. Rutiner vid dataläcka | Vilka lösningar de har |
| 4 GDPR generellt (Forskningsfråga 2) | 1. Tydlighet 2. Användbarhet 3. Brister 4. Begränsning eller möjlighet | Har de en tydlig strategi? |
| 5 GDPR strategi (Forskningsfråga 3) | 1. Utmaningar 2. Kommunikation och samarbete mellan avdelningar 3. Vilka jobbar med GDPR och hur 4. Vem har ansvaret 5. Vilka förändringar de behövde eller kommer behöva göra 6. Implementering och uppföljning | Finns något som GDPR inte skyddar mot? Är det anpassat till IoT och dagens teknik? |
| 6 Övriga kategorier | Intressanta upptäckter | Intressanta aspekter som ej faller inom andra kategorier |

Steg 2.

Potentiella företag och personer som är relevanta för studien valdes ut och kontaktades per mejl. Vid första kontakten informerades alla framtida respondenter om studiens syfte, detaljer om intervjuer såsom längd, etiska riktlinjer och återkopplingsmöjlighet (Bilaga 1). Exempelfrågor skickades till samtliga i förväg, eftersom Denscombe (2016) menar att om respondenterna får tid att förbereda sig på intervjuer genom att få frågorna innan intervjun kan det resultera i mer genomtänkta svar. Eftersom intervjuerna var semistrukturerade, gav det möjlighet till fördjupning i intressanta områden eller att "gräva upp" intressanta svar. De sammanlagt sex stycken intervjuer genomfördes i tre olika organisationer och backas upp med två expertintervjuer. Två av respondenterna arbetar hos samma organisation, men på olika positioner och erbjuder svar utifrån olika perspektiv. Forskargruppen bestod av två personer som turades om vem som skulle intervjua och vem som skulle ta anteckningar och ställa följdfrågor, så att båda forskarna fick genomföra tre intervjuer.

Steg 3.

Transkriberingen av intervjuer genomfördes i direkt anslutning till intervjuer. Alla intervjuer transkriberades ordagrant för att inte gå miste om viktiga och intressanta aspekter. Sammanlagt har ca 3,5 timmar av intervjuer med 24 961 ord transkriberats. En av intervjuerna genomfördes i skriftlig form.

Steg 4.

Intervjumallen användes för att koda intervjuerna.

Steg 5.

Vid kodningen av intervjuer lades fokuset på vad respondenterna sa i ord, inte vad de menade. Vid första kodningen av intervjumaterialet lästes all transkribering noggrant och delades in i passande delar i förutbestämda kategorier. Kodning av intervjuer genomfördes först separat av båda forskare, vilket därefter jämfördes för att säkerställa kategoriernas relevans och tydlighet. Vid avvikande kodning diskuterades vilken kategori ett specifikt svar tillhör enligt överenskommelse. Om det upptäcktes övriga kategorier så adderades dessa till ett separat dokument av respektive forskare för att inte påverka varandras perspektiv.

Steg 6.

Vid baklängesforskningen genomlästes alla transkriberingar med syftet att bredda perspektivet och upptäcka intressanta aspekter utanför de förutbestämda kategorierna. Därefter jämfördes och diskuterades upptäckten. Detta innebär att upptäckter av övriga kategorier och intressanta ämnen verifierades av två forskare. Intervjumaterialet kodades utifrån två forskares olika perspektiv, vilket är ett sätt att uppnå triangulering (Denscombe, 2016).

Steg 7.

Resultatet sammanfattades och presenterades efter första kodningen och baklängesforskningen i en flytande text. Resultatet kategoriserades utifrån teoretiska referensramens grupperingar.

Steg 8.

Efter att resultatet sammanställdes, skickades det till samtliga respondenter för validering för att säkerställa att forskargruppen har förstått deras berättelse korrekt. Endast 4 av 6 respondenter validerade resultatet.

Steg 9.

Resultatet uppdaterades utifrån svar från respondenterna. Respondenterna fick möjlighet att ta bort, utveckla, omformulera eller addera något ytterligare till resultatet. Vid eventuella ändringar skickades resultatet på nytt för en slutlig validering.

2.6 Analysmetod

Enligt Robson (2016) finns inga tydliga och allmänt accepterade uppsättning av regler vid analys av kvalitativ data (vilket samlades in under intervjuerna). Samtidigt menar författaren att det finns metoder för att behandla den kvalitativa datan systematiskt. Tematisk kodning har använts i uppsatsen, vilket enligt Robson (2016) är en realistisk metod eftersom det redogör för erfarenheter och respondenternas verklighet. Datan kodas först och märks.

Därefter kategoriseras data utefter samma märkning under en och samma tema eller kategori. Koder och kategorierna kan enligt boken bestämmas: induktivt från datan och från relevans i forskningsfrågor, tidigare forskning eller teoretiska överväganden. Därefter fungerar kategorierna som grund till fortsatt analys och tolkning genom antingen en beskrivande eller utforskande grund, eller inom en rad teoretiska ramar (Robson, 2016). Den insamlade datan analyserades med teori om informationssäkerhet och integritet (3.1), inställning till och motivation i förändringar (3.2) och teori om implementation av förändringar i samband med GDPR (3.3). Robson et al (2016) påpekar att det finns flera brister med en mänsklig analyst jämfört med en dator, bland annat: insamling av bara positiva instanser, det finns en risk att antingen över- eller underreagera ny information eller att data jämförs med en fiktiv bas. Dessa brister har eliminerats genom att beakta resultat som motsäger hypotesen, att beakta all ny information likadant och att data jämfördes med en teoretisk bas.

Först insamlades en översiktlig litteratur med syftet att orientera sig inom området och därefter specialiserad litteratur för att besvara forskningsfrågorna. Litteratursökningen anpassades i efterhand utifrån relevanta upptäckter. Till all data som samlas in, förhåller sig författarna källkritiskt till och beaktar metodernas både möjligheter och begränsningar.

Wästerfors (2008) resonerar om baklängesforskning. Metoden innebär att man går genom det insamlade materialet och funderar på vilka frågor det besvarar istället för att använda den traditionella metoden och försöka hitta svar på existerande frågor. Wästerfors (2008) och Gioia (u.d.) menar att vid induktiv forskning kan det vara fördelaktigt att börja med datainsamling och dess analys innan man fördjupar sig i existerande forskning. Detta på grund av att kännedom av forskning kan begränsa tankesättet och kreativitet i analysen. Insamling av relaterad forskning påbörjas därför i de första faserna men kompletteras efter datainsamlingen för att ge möjlighet att analysera upptäckter som kommer upp i resultatet.

2.7 Etiska riktlinjer

Datainsamlingen skedde i enlighet med Vetenskapsrådets (2017) etiska riktlinjer och därför samlades ett informerat samtycke (Bilaga 2) från respondenterna innan intervjuerna påbörjades vilket innehöll en introduktion om att deltagandet är frivilligt, information om intervjuens varaktighet och sekretess. Samtidigt fick respondenterna chans att ställa ytterligare frågor om forskningen och hur svaren skulle användas. Respondenterna hade ingen tystnadsplikt men för att värna om deras konfidentialitet genomfördes intervjuer med en person i taget och intervjuobjekten anonymiseras. Respondenterna fick även möjlighet till återkoppling och validering av sina svar.

2.8 Källkritik

Följande nyckelord användes för att finna relaterad forskning inom området: “vulnerabilities”, “smart camera”, “GDPR”, “IoT”, “privacy by design”, “motivation”, “förändringar”.

Kriteriet vid sökning av litteratur var att alla källor skulle vara referentgranskade och detta eftersträvades så gott det gick. Tyvärr är området väldigt nytt. GDPR hade ännu inte trätt i kraft när uppsatsen och litteratursökningen påbörjades. På grund av detta fanns det en del material som inte uppfyllde det ovan nämnda kriteriet men användes ändå i brist på andra källor. I dessa fall gjordes en avvägning om källan gick att lita på och endast källor som godkändes i avvägningen användes i uppsatsen. Förutom artiklar och andra digitala källor användes även böcker. Även här gjordes en utvärdering av deras pålitlighet. Utvärderingen

omfattade författaren och vilken erfarenhet denne har inom ämnet, källans äkthet, dess budskap, presentationen, datumet för publikation och den allmänna uppfattningen av trovärdigheten. Ovetenskapligt material som webbsidor endast användes i Kapitel 1, Introduktion i syfte att belysa och presentera områdets popularitet och relevans till läsaren.

2.9 Triangulering

Triangulering inom samhällsforskning betyder enligt Denscombe (2016) att man undersöker problemet ur flera synvinklar eller hämtar information från flera källor för att öka validiteten. Detta kan göras på olika sätt. I denna uppsats görs källtriangulering (genom att personer från olika positioner, företag och med olika perspektiv intervjuas), observatörstriangulering (genom att båda forskarna medverkar i alla intervjuer och kategoriserar resultatet), samt analystriangulering (genom att resultatet först kategoriseras och sen används baklängesforskning).

3. TEORETISKT RAMVERK

I detta kapitel presenteras till studien relevant teoretisk referensram uppdelad i tre delavsnitt. Avsnittsuppdelningen utgår ifrån forskningsfrågorna. 3.1 behandlar teorier inom ramen för delfråga 1, 3.2 används för delfråga 2 och 3.3 till att presentera teorier kopplade till delfråga 3. Innehållet i avsnittet är grunden till empirin, samt analysen och syftar till att synliggöra kopplingen mellan empiri och analys.

3.1 Informationssäkerhet och integritet

Enligt O'Brien (2016) föreskriver GDPR-krav för datakontrollant-företag som har en direkt relation till användare och leverantörer som är dataprocessorer. Svaret på hur mycket säkerhet som behövs enligt Sherwood et al (2005, 4) beror på värdet av det som skall skyddas och på den operativa risken. Samtidigt hävdar Carroll et al (2012) att det inte existerar ett pålitligt sätt att bestämma hur säkert ett system är eller att kvantifiera en organisations hållning till informationssäkerhet. Genom operativ riskhantering (operational risk management) identifieras hot, analyseras sårbarheter och mitigeras riskerna.

Enligt O'Brien (2016) bör informationssäkerhet betraktas utifrån ett holistiskt perspektiv tillsammans med utbildning och medvetenhet, fysisk säkerhet och "due diligence" på tredje parter inklusive kontraktskrivning. Utöver det föreslår O'Brien specifika kontroller i form av en riskhanteringsprocess. O'Brien (2016) menar att traditionellt är säkerhet placerad inom IT avdelningen och integritet ses som en juridisk fråga och hanteras av en juridisk avdelning, men enligt honom: "*Acting in isolation, neither can be effective*". The evolution of information assurance (2002) styrker O'Briens teori men artikeln säger att applikationer själva kommer aldrig kunna hantera alla säkerhetskrav, därför kan integrering av säkerhetsfunktioner i enheter förbättra systemets säkerhet. Säkerhetsfunktionalitet bör distribueras mellan fysiskt distinkta komponenter, så att dessa själva kan skydda sina kritiska resurser.

Enligt Sherwood et al (2005, 1) adderas säkerhet ofta efter implementering och efter att en incident inträffar, vilket innebär att informationssäkerheten således är isolerad från affärsprocesser. Sherwood et al (2005, 29) menar vidare att det är nödvändigt med en helhetssyn på säkerheten. Sherwood et al (2005, 29) anser att användning av en checklista misslyckas, eftersom fokuset ligger då på att kontrollera varenda del för sig istället för helheten och om en del saknas, kan det resultera i att alla andra delar blir värdelösa.

Samtidigt menar O'Brien att GDPR bara är en grundlösning (bottom line), eftersom de GDPR notifieringskraven (notification requirements) som finns bara säger att någon råkade ut för en incident. Men företagen enligt O'Brien måste själva inkludera datakategorier, posterna som berörs och delen av dataområdet som är påverkat, vilket innebär att företagen måste tillhandahålla detaljerad intelligens om vad en hacker eller anställda har gjort.

Enligt O'Brien (2016) kräver GDPR en mer grundlig dokumentation av företagets aktiviteter och att samtidigt skapa bevis om en proaktiv "privacy by design" planering i sina aktiviteter.

3.2 Inställning till och motivation i förändringar

Arbetsuppgifter kräver enligt Jacobsen och Thorsvik (2008, 294) samarbete, koordinering och kommunikation av information. Avsaknad av information kan vara en orsak till frustration och bristande motivation hos medarbetare (Jacobsen och Thorsvik, 2008, 294).

Sandholm (2012) menar att förändringar kan upplevas som ett hot av människor, vilket kan resultera i motstånd mot förändringar. Enligt Sandholm (2012) kan motsättningar visa sig varierande, exempelvis genom förträngning, vägran eller att människor låser sig vid sina egna uppfattningar. Undvikelse av motstånd kan enligt Sandholm (2012) ske genom att exempelvis erbjuda deltagande och tillräckligt med tid för accepterande.

Lagar och förordningar har stor betydelse och påverkanskraft för företag. Enligt Jacobsen och Thorsvik (2008) om organisationer inte tar hänsyn till lagar och bestämmelser kan det resultera i legitimitetsproblem mot företagets omvärld, vilken försvagar organisationens rykte och även resulterar i bestraffning. Zerlang (2017) menar att det nu är upp till företagen om de väljer att dra nytta av förändringen som GDPR medför genom innovativa teknologier, eller om de istället väljer att betala höga böter. Som tidigare nämndes menar Junwoo et al (2017) att IoT företagens kostnader kan tre- eller fyrdubblas i följd av dataskyddsförordningen. Enligt Junwoo et al (2017) visar statistik att GDPR ökar spänning och orolighet hos företag då mer än hälften är oroliga för böterna och funderar på att byta sina affärsstrategier.

Utanför företagets gränser är det enligt IT Governance Team (2016) viktigt att förstå att relationen med andra aktörer kan innebära en sårbarhet vilken oftast löses genom kontraktskrivning om att ens data är säker hos det andra företaget.

3.3 Implementation av förändringar i samband med GDPR

Enligt Zerlang (2017) kommer företag generellt bli tvungna att öka säkerheten i sin data, system och processer vid moderna teknologier genom säkerhetsinformation (security information) och händelsehantering (event management) som blir möjliggörare för att överensstämna GDPR.

En planerad förändring enligt Jacobsen och Thorsvik (2008, 426) kräver tre element: ett tydligt mål, säker kunskap (om förändringens behov, lösningar och åtgärdernas effekter) och en lyckad implementation av förändringen enligt planerna. Vidare nämner Jacobsen och Thorsvik (2008, 431) att en organisationsförändring inte bara påverkar organisationen internt, men att det även innebär nya förhållanden till externa parter. Påståendet kan understrykas genom Lindqvists (2017) uttalande om att en kontinuerlig kontroll av befintliga och kommande kontrakt mellan IoT intressenter är nödvändigt. Att involvera medarbetare i förändringen har enligt Sims (2002) en positiv påverkan på implementeringens framgång.

Enligt Borglund et al (2012) kan organisationer vinna förtroende på fyra sätt: transparens av relevant information, visa sin kompetens, följa riktlinjer och genom att visa välvilja mot andra. Som tidigare nämndes (3.2) brukar kontrakt användas för att säkerställa att data är säker utanför företagets gränser. Men kontrakt ger ingen riktig försäkran om att exempelvis leverantörer följer godkända processer. Borglund et al (2012) menar samtidigt att organisationer genom att certifiera sig kan kommunicera sitt ansvarstagande till sina intressenter. Därför kan en lösning vara att kräva ISO 27001 certifiering från sina leverantörer (IT Governance Team, 2016).

Vidare nämner Jacobsen och Thorsvik (2008) att en strategi för att upprätthålla en organisations legitimitet kan ske genom berättigade metoder som exempelvis målstyrning eller kvalitetssäkring. O'Brien (2016) menar dock att bredden av förändringar som måste göras för att uppfylla GDPR-kraven är väldigt betydelsefull och menar att företagens snabbhet och förmåga är beroende av företagets integritetsmognad.

Zerlang (2017) poängterar att omvandlingen kommer att kräva en betydande planering och granskning kring människor, system och processer nödvändiga för att garantera säkerhet inom organisationen, vilket O'Brien (2016) förstärker med sin synpunkt om att företagsledningen behöver få specifik utbildning samt att de behöver säkerställa att specifika planer är införda för att säkerställa kravens uppfyllelse. Utöver det menar O'Brien (2016) att den första och viktigaste uppgiften för organisationer är att säkerställa att GDPR ämnet visas i ledningsagendan (management agenda) och att medel är allokerade till specifika lösningsprogram.

Enligt Zerlang (2017) kommer implementering av förändringen bli en utmaning i organisationer som enbart fokuserar på att överensstämna med GDPR-kraven och tillägger att det blir en utmaning att bryta ned siloerna i processen vid de givna kraven. O'Brien (2016) menar då att konsekvensbedömning (privacy impact assessment) och att företag inkluderar integritet genom design (privacy by design) i vanliga företagsaktiviteter och processer är viktigt, vilket ligger i linje med en proaktiv informationssäkerhets riskhantering. Tankard (2016) tillägger att datakryptering och pseudonymisering är lämpliga skydd för att säkra data så länge det inte är möjligt att koppla data till en specifik individ.

GDPR kräver att företag ber om informerade samtycken från användarna, vilket enligt Niese et al (2016) är komplicerat eftersom IoT anordningar saknar tillräckliga användargränssnitt för att förse användarna med informerade samtycken och det förekommer olika uppsättningar data som kan behöva ha olika inställningar till informerade samtycken. Niese et al (2016) tillägger att informerade samtycken enligt GDPR behöver samlas in innan IoT apparater kommer till användning och börjar samla in data. Utöver det menar författarna att databehandling är rättslig enligt GDPR, bland annat: om samtycke ges av användare, om databehandling är nödvändig för att verkställa ett kontrakt där användaren är en part eller om behandling av data är väsentlig för att skydda användarens vitala intressen. Niese et al (2016) tillägger dock att det enda sättet att behandla data på ett rättvist sätt är genom samtycken. Samtidigt får inte samtycket bli stoppande, vilket enligt Niese et al (2016) kan lösas genom tydliga och medvetna policy beskrivningar.

Zerlang (2017) menar att utnämningen av Data Protection Officer (DPO) presenterar ett erkännande hos företagen om att data är ett centralt element för organisationens framgång. Vidare nämner Zerlang (2017) att det är DPO:n som kommer att tillhandahålla företaget med en holistisk översikt över vilka data företag behandlar.

Long (2017) anser att många företag inte förstår hur djupt in i företaget som de behöver göra förändringarna på grund av GDPR och menar att de flesta ganska fort inser att dataskyddsförordningen har en signifikant påverkan på alla delar av organisationen. Lindquist (2017) påpekade en problematik kring upprättning av kontrakt mellan intressenter, eftersom flera olika parter är involverade i ett IoT sammanhang. Enligt Lindquist (2017) kan detta leda till förvirring bland företag.

4. EMPIRI

Här presenteras resultatet av det insamlade materialet från intervjuerna vilket används i analysen för att besvara forskningsfrågorna. Som tidigare beskrivits är respondenterna anonymiserade och förkortas som R.

Underkategori 1 kommer att besvara delfråga 1, underkategori 2 kommer att ge svar på delfråga 2 och underkategori 3 kommer besvara delfråga 3. Empirins delkategorier presenterar relevanta områden som respondenterna uppmärksammade under intervjuerna och grupperade ämnesvis. Intervjumallen bifogas som bilaga 3.

4.1 Informationssäkerhet och integritet före GDPR

4.1.1 Dagens tillstånd

R2 berättade att om det går ett brandlarm, skickas den signalen upp till larmcentralen och lagras. I appen finns dessutom enligt respondentens berättelse t.ex. temperaturdata och historik om användarnas hem, vilket innebär att företaget hanterar både temperaturdata och historik. R4 berättade att datan företaget behandlar har en kort livscykel. Bilder på hemmet tas enligt respondentens berättelse när något ovanligt utlöser larm, vilket skickas till larmcentralen för en verifiering. Bilder sparas högst 30 dagar efter händelsen, annars raderas bilderna automatiskt. Dessutom behandlar R4s företag information om vilka kameror en kund har och för att kunna skapa access och konto behövs användarnas förnamn, efternamn, epost och mobilnummer. R5 påpekade att för att möjliggöra IoT behövs data. Alla IoT produkter involverar någon typ av persondata till viss del enligt R5, vilket innebär att företaget därför automatiskt omfattas av GDPR.

R2 berättade att det inte finns data i deras produkt, utan att data förvaras i en databas. I produkten står det endast "användare 3". Respondenten tyckte att denna lösning är obetänksam:

"Det inte har med GDPR att göra, utan det är en dum lösning." (R2)

R4 sa att video lagras i larmcentral eller hos kunden. Andra respondenter har inte berättat om hur deras företag förvarar data.

R1 sa att företaget uppdaterar var tredje månad sina produkter med funktions-förbättringar. Äldre produkter enligt respondentens berättelse uppdateras reaktivt vid buggar av en annan avdelning på företaget. R2 berättade att de släpper ny mjukvara kanske varannan, var tredje vecka men inte till alla sina kunder.

"Vi har en policy att ingen kund ska ha en mjukvara som är äldre än 1 år. Kan rulla ut mjukvara till alla på kanske 1 vecka eller 2 vid något allvarligt." (R2)

Det löser företaget genom att använda ett verktyg som kan uppdatera mjukvaran hos alla, utan att kunderna märker något. Det körs i många fall via cellulära nätverk och företaget betalar för datakostnader. Enligt R2 patchar därför företaget inte till alla kunder hela tiden, utan endast då något allvarligt inträffar och en gång om året. R4 jobbar på ett företag där dotterbolagens tekniker utför uppdateringarna, vilket enligt personen kan göras på avstånd. R4 berättade att allmän systemomfattande service görs 5 gånger om året.

R1 berättade att vanliga funktionella buggar åtgärdas enligt ticketsystem. Företaget försöker släppa mjukvara var tredje månad men vid allvarliga fel görs en allvarlighetsbedömning och uppdateringen skjuts upp. Vid hög allvarlighet görs "vulnerability board". Att fixa det går enligt personen ofta snabbt, men att få kunder att installera uppdateringarna är en utmaning. Många kunder är enligt R1 inte uppkopplade på internet eller tillåter endast mjukvara som har varit felfri i 6 månader.

"Det finns inbyggda långsamheter. Det är dyrt för många företag att byta och uppdatera mjukvara." (R1)

R2 sa att buggar brukar upptäckas vid penetrationstest men företaget har kunnat åtgärda säkerhetsbrister innan någon har märkt det. Annars lägger företaget en buggrapport på den delen vilket först lagas och därefter "patchas" det ut till kunderna efter att de lagat hålen. Om det är ett fel på servern, så rullar företaget ut patcharna till alla sina kunder så alla får det på en gång. Enligt respondentens berättelse hittills har företaget inte upptäckt något så allvarligt att de behövde uppdatera alla på en gång. R3 bekräftade det som R2 berättade, eftersom personerna som tidigare nämndes arbetar hos samma företag. R6 ansåg en utmaning med att:

"Det är svårt att veta hur mycket är tillräcklig säkerhet. Säkerhet är dyrt, det kräver specialkunskap." (R6)

4.1.2 Säkerhet

R1 arbetar hos ett företag som inte är kravspecifikation fokuserat enligt respondenten. Företaget försöker komma bort från att jobba utifrån kravspecifikationer, eftersom de anser att det inte leder till det bästa resultatet. Men utifrån ställer marknaden specifika krav, inifrån företaget finns det en annan sorts krav som inte är formaliserade enligt R1. Utvecklingsstrukturen är modellerad efter open source plattformen, med CBM:er (code block maintenance) vilket säkerställer säkerheten. R1 tyckte att det är en stor risk för företaget om kunderna inte uppdaterar och därför är sårbara. Därför går företaget enligt respondenten mot en uppkopplad värld för att samla in system-data (som inte är integritets betungad) för att kunna mäta hur deras produkter mår, vilka versioner och problem produkterna har. R2 och R3 beskrev däremot att företaget de jobbar hos arbetar utifrån dokument som beskriver hur protokollet ska se ut och hur allt ska säkras. All persondata "scramblas" redan när den används i produktionen. Därefter utför externa team "penetrationstest" och utför tester för att se till att riskerna mitigerats.

R4 beskrev att det utförs backup flera gånger per dygn, för vilket dotterbolagen själva ansvarar. Enligt R4 görs det backuper även på de centrala systemen. Företaget arbetar med Active Redundance och använder därför 2 servrar plus ytterligare backup på dessa. R4 beskriver sitt företag som ganska rustat när det gäller säkerhetslösningar eftersom företaget använder sig av lösenordskydd där systemet märker upprepade inloggningsförsök. Utöver det krypteras all data som förekommer och företaget har ett eget nät med ett starkt krypto. Det fysiska skyddet består av loggning av personer, inpasseringssystem och passagekort.

R5 talade om att många utvecklare inte är tränade inom säkerhet. Vidare tillade personen att det behövs speciella kunskaper för säker kodning. R5 påstod att säker kodning är inget man lär sig i skolan och menar att:

"Nu är det svårare, eftersom det måste identifieras var datan finns och problemet uppkommer om den är spridd överallt." (R5)

R6 ansåg att företag inom säkerhetsbranschen förmodligen är mer förberedda och kommit längre med GDPR än företag som verkar inom andra branscher. R6 la till att företag ska ha tillräcklig säkerhet för att skydda personuppgifterna de behandlar och framhävde att om information om till exempel statistik överförs till supporten i Indien så måste det finnas något som ser till säkerheten, i annat fall kan informationen användas till att exempelvis bryta sig in i kundens hem.

R2 uppgav att dataläckor inte har inträffat på företaget personen jobbar hos, vilket R3 betygade med att vid en eventuell dataläcka skulle företaget nyttja de processer de har för att hantera likartade händelser. Företaget implementerar ISO 27001 just nu, vilket företaget hämtar policys och processer ifrån. R4 berättade att vid en eventuell händelse utförs det en undersökning först vilket följs av en konsekvensbedömning.

4.1.3 Dataintegritet

R1 berättade att företaget hanterar ingen data vid utveckling. Datahantering finns främst i drift och företaget driftar i huvudsak inte, utan säljer till ett annat företag som kombinerar och säljer en helhetslösning. Det finns dock enligt respondenten områden som hanterar data men respondenten gav ingen beskrivning om vilka dessa områdena är, men tillade att det finns ett system som driftas men personen kan inte svara på hur det hanteras. R2 menade att det finns flera olika nivåer kopplade till hela flödet. Det finns även regler i larmbranschen som fungerar likadant för alla larm. Enligt respondentens exempel loggas det varje gång larmoperatören tittar på bilder och att de bara kan komma åt bilderna om det har uppstått en incident. R5 menade att integritet är väldigt komplicerat och annorlunda från säkerhet. R5 la till att integritet även skiljer sig mellan länder.

Varje respondent upplyste om diverse lösningar. R2 klargjorde att alla avdelningar har sina egna policys om dataintegritet, beroende på vad en specifik avdelning gör. Organisatoriskt håller enligt respondenten säkerhetsavdelningen reda på policys, men tillägger att det inte händer att någon överordnad granskar deras dokument som de själva håller koll på. R3 berättar att personens företag tittar extra noggrant på vilken data som processas utifrån ett integritetsperspektiv.

R4 beskrev vilka personer som har tillgång till bilder: larmoperatörer, teknikerna vid konfigurering och att kunder själva kan få åtkomst till sina bilder. Därefter beskrev R4 att bilderna raderas automatiskt från systemet men att pågående brottbilder sparas i högst 30 dagar. Bilderna tas enligt respondenten bort kontinuerligt. R4 poängterade att termiska kameror inte ser ansikten, till skillnad från optiska.

R5 hävdade att det krävs en stor förändring i hela företaget för att uppnå "privacy by design", eftersom enligt personen måste alla på företaget förstå vad persondata är. R5 föreslog att börja med att hitta vilken persondata som finns i företaget och därefter implementera säkerhet. Utöver det nämnde R5 att det krävs en kultur från VD:n hela vägen ner, medvetenhetssessioner, utbildningar och planerade tester. R5 betonade att det bästa lösningen är att inte samla in någon persondata alls.

Endast R6 nämnde någon risk kopplad till dataintegritet. Personen berättade att det nästan aldrig kan garanteras att datan är anonymiserad, eftersom den kan jämföras med en annan databas och då kopplas till specifika individer.

4.2 Anställdas inställning till och förståelse för GDPR

4.2.1 Tydlighet

Fyra av sex respondenter tyckte inte att GDPR är tydligt beskriven. R1, R3, R4 och R5 ansåg att definitionen av persondata är väldigt bred i GDPR vilket gör beskrivningen väldigt svårtolkad. Enligt R1 och R3 är det därför svårt att veta vad som är rätt tolkning och vad som räknas som känslig information. R1 och R3 tyckte dessutom att det är svårt att veta hur GDPR praktiskt skall åstadkommas rätt och enligt R3 all initiativ till att bli kompatibel blir allt större och svårare. R1 beskrev att det är en utmaning att tolka GDPR rätt och att exempelvis kryptografi eller pseudonymisering (en procedur av avidentifiering, där datafält byts ut mot pseudonym, vilket gör data mindre identifierbar) inte löser integritetsproblem men är ändå rekommenderat i GDPR, vilket gör det otydligt om det måste användas eller inte och vilka effekter dessa val har. R5 tyckte att det är otydligt om det behövs en DPO i företaget eller inte. Enligt R4s berättelse är rollerna inom GDPR otydliga och det är svårt att veta vad som är rätt eller fel tolkning:

“Vem är datakontrollant? Är företaget processor gentemot kunden och kunden är kontrollant?” (R4)

Enligt R5 och R6 berättelse förklarar inte GDPR vilken typ av säkerhet som behövs. R6 menar att GDPR bara säger “tillräcklig säkerhet”, inte exakt vad och hur. Enligt R6 finns:

“...inget system för att klassificera hur man gör, det är upp till företagen att göra riskbedömning.” (R6)

Vilket enligt R6 är lite godtyckligt, eftersom det är upp till företagen, men vilket sedan bedöms av ett annat organ huruvida det var tillräckligt ifall någonting händer.

Enligt R6 är GDPR i sin helhet är ganska tydlig, men berättade att utifrån sin erfarenhet tycker företag att det är otydligt. Enligt R6 saknas officiell information från EU och att det är för sent med information som har börjat komma från Article29 Group, eftersom GDPR träder i kraft i maj 2018. Vad gäller tydlighet mot användarna tyckte R1 att det finns en risk att användarna kommer acceptera avtal som de inte förstår.

4.2.2 Användbarhet

Enligt R3 täcker GDPR mycket runt integritetsfrågor, vilket enligt R5 är ett steg i rätt riktning eftersom det höjer uppmärksamheten runt integritet samtidigt som den ger den individuella användaren rätt till sin data. R5 la till att det blir intressant att se hur dataskyddsförordningen kommer att utvecklas, eftersom ingen riktigt vet för tillfället. Men enligt R5 är GDPR bara “baslinjen” inom säkerhet. Enligt R6s berättelse saknas det riktlinjer, förslag och fler rekommendationer inom GDPR och tillägger att det vore uppskattad med konkreta exempel. R6 lade till att:

“Nu jobbar alla företag med det för att de måste” (R6)

R4 berättade om en annan svårighet inom användbarhet vilket är just de alldeles för många avtalen som personens företag måste upprätta, vilket uttrycktes enligt följande:

“Sen alla vill använda standardavtal därför har vi 6-7 olika avtal. Den centrala IT av företaget ska ha cirka 150 avtal... Det var en överdrift från min

sida, men det blir ganska många avtal. Vore bra med standardavtal från EU”
(R4)

R2 berättade att GDPR arbetet för andra avdelningar är mer omfattande än för sin avdelning, då avdelningen personen arbetar på använder sig av knappa personuppgifter:

“För massa andra människor är det ett jättestort jobb men ganska skonsamt för mitt team. Vi håller ingen data. Kan endast hända att vi använder någonting felaktigt i utvecklingsmiljön.” (R2)

Enligt R5 berättar GDPR bara om principer och vad som måste åstadkommas, men inte hur det ska implementeras vilket faller inom både Användbarhet och Tydlighet kategorier. Enligt R1 och R6:s berättelse fungerar dataskyddsförordningen inte helt säkert inom industrin:

“hur kan man ha avtal med alla parter på en allmän yta, exempelvis?” (R1)

R6 undrade:

“vems personuppgifter det är egentligen? Är det personen som har fått den att bli installerad i sitt hus, eller är det personerna som bilderna är tagna av?”
(R6)

4.2.3 Brister

Tre av sex respondenter uttryckte flera brister inom GDPR. R4 poängterade att på grund av “undantagen” inom GDPR finns det en del luckor vilka företag kan gå runt och R4 menar då framförallt möjligheten till att be om samtycke:

“...bara med samtycke kan man nästan göra vad som helst” (R4)

Enligt R5 adresserar GDPR integritet, men inte säkerhet. Personen tyckte att GDPR saknar detaljer i sin beskrivning. Personen trodde till och med att det kanske kommer en uppdatering av förordningen.

“Man behöver kompletterande material för att använda GDPR så det kanske kommer en ny version av den.” (R5)

R5 berättade att GDPR rekommenderar till exempel anonymisering av persondata, men att just anonymisering enligt respondenten kanske inte är tillräckligt. Personen i fråga uttryckte sin skepticism om hur dataskyddsförordningen kommer att följas upp och hur det kommer säkerställas att sekundär användning av data inte förekommer.

Enligt R6 har informationen om att företag måste ens verkställa någonting varit bristfällig. Utifrån R6:s erfarenhet har de företag som jobbar med mjukvaruutveckling rätt bra koll på förordningen, men inte företag i andra branscher. En annan brist i GDPR som R6 påpekade är att företag har möjlighet att dölja om något hade läckt genom att hävda att data har läckt säkert. Vidare nämner R6 att dataskyddsförordningen kan ha påverkan på tillverkningskostnader, eftersom enligt R6 är säkerhet dyrt. Enligt R6 kan det förekomma att företag köper hårdvara av sämre kvalitet som kanske inte klarar av kryptering eller har lite minne, vilket innebär i slutändan lägre säkerhet. R6 ansåg att det kan därför bli dyrare för konsumenten att ha bättre säkerhetsstöd i framtiden.

4.2.4 Begränsning eller möjlighet

Tre av sex respondenter; R1, R4 och R6 är överens om att GDPR är en möjlighet för företaget, men ibland är en begränsning. R1 anser personligen att dataskyddsförordningen är ganska bra, eftersom företagen tvingas hantera integritetsfrågor medvetet. Enligt R1 innebär GDPR en möjlighet till företag att åstadkomma det bättre än konkurrenter, vilket R6 förstärker med sin berättelse om att GDPR innebär en möjlighet till att bygga företagets varumärke:

“... möjlighet till att marknadsföra sig med att visa att man tänker på sin kund... kunden är viktig.” (R6)

Men både R1 och R6 tycker samtidigt att GDPR är en begränsning:

“I vissa tillämpningar sätter käppar i hjulet. Klurigt hur tjänster ska byggas upp och vem som ska ta ansvaret.” (R1)

“Begränsar vad företag vill göra.” (R6)

R4 ansåg att dataskyddsförordningen inte är farligt för de, men samtidigt är det en belastning då avtalen med leverantörer måste skärpas, men personen tycker att efter avtalen är upprättade innebär inte GDPR någon större belastning eftersom många av GDPR-kraven har personens företag redan uppfyllt. R4 menade att dess företag inte använder data som de behandlar till något annat, eftersom:

“Den datan vi har behöver vi bara för att hantera larm.” (R4)

R6 berättade om vissa delar av databehandling läggs ut till ett annat företag, då skall datakontroller och dataprocesser företag enligt GDPR upprätta ett avtal mellan varandra.

Enligt R6 innebär GDPR en möjlighet till att få företag att jobba med säkerhet, som personen beskrivit enligt följande:

“En liten ursäkt att komma igång, oftast gör man inte det.” (R6)

Därefter la R6 till sin berättelse att utifrån sin erfarenhet märks nu lite panik bland företag för att GDPR är en omställning och en stor förändring för hela industrin. Många börjar anpassa sig först nu (två månader innan GDPR träder i kraft), men många företag har samtidigt inte förstått att GDPR kräver ett kontinuerligt arbete:

“Vissa förstår inte att detta inte är en engångsgrej.” (R6)

4.3 Implementation av förändringar i samband med GDPR

4.3.1 Utmaningar

R1, R2 och R3 uttryckte att otydligheten i vad som är okej och inte okej enligt GDPR och konsekvenser av dessa är en utmaning.

“Man vet inte förrän det har testats i rätten och utfallet därifrån. Risken är att man missar någonting.” (R1)

“Det finns en utmaning i att tolka gdpr rätt.” (R3)

R3 ansåg att awareness skulle bli en utmaning och att få anställda att förstå allvaret i GDPR. R3 ansåg att anonymisering/pseudonymisering av intern data är svårt praktiskt och enligt personen kan det vara nödvändigt att ha extra funktioner. Respondenten tillade i sin berättelse följande:

“Man behöver hitta ny lösning för varje scenario.” (R3)

Enligt R4 är det tidskrävande att skriva nya avtal för varje underleverantör. R4 framförde ytterligare att det hade underlättat med en standardavtal från EU. Förutom avtalen ansåg R4 en annan utmaning: att tala om en dataläcka inom 72 timmar, då det enligt personen påverkar varumärket och aktiekursen negativt plus att företaget kan få betala höga böter. R1 delar R4:s syn, eftersom respondenten förklarade att vid en allvarlig händelse består “vulnerability board” av bland annat PR-människor som tar hand om kommunikation utåt vid en eventuell dataläcka. R4 ansåg att det är väldigt känsligt att tala om när en dataläcka har skett på grund av konsekvenserna.

R5 sa att en utmaning kan vara att visa integritet meddelande eftersom smarta kameror inte har någon skärm:

*“Hur presenterar man det då om GDPR kräver det? Finns sätt att undvika det på, man kan delegera det till en annan enhet, t.ex. en mobil men inte alla produkter stödjer det. De som har låg processorkraft, som är billiga stödjer inte interoperabilitet. Många är också autonoma och kommunicerar själva. Ska kundens samtycke ges hela tiden, 24*7*7 timmar?” (R5)*

En annan utmaning enligt både R5 och R6 är att ta bort användarnas data om de begär det. Det är osäkert enligt respondenten hur företag hanterar data och hur de lyckas ta bort den inom 72 timmar. De måste därför enligt respondenten vara medvetna om var data samlas, omvandlas, kopieras, nämligen hela livscykeln.

“Det finns inte så mycket forskning inom det. Men även i praktiken, tas data bort från kopior? Användaren kommer inte veta det.” (R5)

Om det finns avtal, användarvillkor och alla fina dokument så följer man reglerna men implementeringen i praktiken är en annan sak enligt R5 som samtidigt menar att företag måste göra en avvägning mellan användbarheten och integriteten. Enligt R5 hanteringen av GDPR är väldigt invecklad:

“Hur tränar man DPO:n? Även erfarna utvecklare verkar inte veta hur de ska hantera GDPR och kunde inte hitta information om det. Vissa har inte resurser för att anställa säkerhetsexperten, så då kanske en utvecklare blir DPO. Det kan utgöra ett problem.” (R5)

Samtycken enligt R6 berättelse måste vara specifika, inför exempelvis varje ny funktionalitet. Samtidigt får samtycken inte stoppa kunden från att använda tjänsten:

“Samtycken får inte bli stoppande, kunden ska få använda tjänsten om det är tekniskt möjligt. Det sker mycket förändring “bakom” kameran.” (R6)

GDPR gäller för tidigare insamlad data med och då kan företag antingen be om samtycke eller radera datan. R6 berättade att samtycket skall samlas in strax innan insamlingen av

datan, vilket kanske ska lösas med en app eller webbtjänst där kunden kan aktivera produkterna och samtycka. Viktigt enligt R6 är att kunden aktivt måste ge sitt samtycke till företaget. R6 undrade:

“Hur hanterar man email? Vems personuppgifter är det om det tas bilder på en tjuv till exempel?” (R6)

R1 tyckte att det ska bli väldigt spännande framförallt i molnsystem, eftersom molnleverantörer beskriver var de förvarar data, men enligt respondenten om någon tittar noga så kan man få känslan av att de skjuter över ansvaret på den som gör sluttjänsten.

“Spännande vem det är i slutändan som tar hand om ansvaret för hur det kommer bli.” (R1)

R4 nämnde att man även kan argumentera för att kunden är kontrollant, vilket i sin tur också kan kopplas till 4.2 Tydlighet kategorin.

4.3.2 Kommunikation och samarbete mellan avdelningar

R1 berättade att en legal avdelning finns och kan rådfrågas vid eventuell tveksamhet. R2 sa att de anställda som sitter nära stackmässigt sitter nära även fysiskt, på samma våningsplan och att de hjälper varandra. Samtidigt menade R2 att så fort det föreligger ett fysiskt avstånd så blir det svårare att samarbeta. Respondenten fick inte mycket återkopplingar på ändringar som behöver införas från GDPR-gruppen.

“De intervjuade mig, så sa de bara, ”jaja, vi får se om vi hör av oss” och så gick de igen.” (R2)

4.3.3 Vilka arbetar med GDPR och hur?

Hos varenda studieobjekt arbetar en större grupp av personer specifikt med att genomföra förändringar som GDPR för med sig. Säkerhetsgruppen på R1:s företag försöker skapa en utvecklingsmodell vilken kommer att handleda utvecklarna, eftersom enligt respondenten behöver alla som arbetar med utveckling besitta en viss förståelse för GDPR. Enligt R1 arbetar specifika grupper med att dokumentera. R2 berättade om att det finns ett team som jobbar med GDPR på företaget som utfört intervjuer med alla anställda om hur de jobbar och vilken data de har. R2 tyckte samtidigt att det är IT development och driftavdelningen som påverkas mest av förändringar. R3 bekräftade R2:s berättelse om att det finns en grupp som arbetar med att tolka, driva och implementera ändringar i alla system. R4 berättade att varje dotterbolag har sitt “gäng” plus juridisk expertis som specifikt arbetar med GDPR. Det är GDPR gruppen som utför kartläggning av all persondata företaget kontrollerar. Företaget jobbar nu (vid intervjuens tidpunkt och enligt R4) med att säkerställa att administrering av kunderna blir rätt, samt har företaget även anställt leveransstöd för GDPR (konsult). R6 föreslog implementering av ISO 27001 säkerhetscertifiering för företag vilket innehåller både tekniska och organisatoriska bitar: ISO 27001 är samtidigt erkänd av GDPR.

Varje företag som intervjuades kommer att vara försedd med en personuppgiftsansvarig. R5 nämnde att DPO:n ska vara den ansvarige som anställda ska kontakta vid eventuella frågor. R6 förklarade att personuppgiftsansvariga har rollen som kontroller och det är även den personen som verkställer samtycke med kunder.

4.3.4 Vilka förändringar behöver göras?

R1 berättade om att företaget frivilligt håller på med ISO 27001 certifiering och att företaget även inför en utvecklingsmodell som har med säkerhet att göra. Utvecklingsmodellen skall enligt respondenten fungera som en lathund och företaget beaktar GDPR som ett hot i hot-modelleringen:

“Där ingår hot-modellering med GDPR som ett hot. Det införs dataklassificering i förhållande till privacy. Företaget tog fram best practice till hur man ska hantera olika typer av dataklasser och data inventory med vilka typer av data företaget hanterar. Detta är inte helt på plats än. Det handlar om att populera den i efterhand.” (R1)

R2 sa att det inte har gjorts några förändringar än, till respondentens kännedom. Enda förändringen är att börja låsa in alla CV, men enligt respondenten så kommer det att komma mer förändringar. Vid intervjuens tidpunkt kände R2 inte till vilka förändringar som behöver implementeras:

“GDPR-gruppen har bara inte kommit ut med resultatet än. Oklart när det händer. Tror det följs redan ganska bra men osäker på produktionsmiljöer. Kommer finnas många ändringar där. En kund ska kunna begära ut all data men backenden löser det.” (R2)

R3 berättade att företaget implementerar ISO 27001, samt har dedikerad personal som på heltid implementerar förändringar och processer. Utvecklingsprocess enligt personen träffas mest av “privacy by design” därför behövs inte mycket förändringar just i utvecklingen. Företaget tittar nu på vilken data som produceras och vad de ska göra ur integritetsperspektiv. R4 berättade att det inte finns mycket förändringar de behöver göra, förutom att dokumentera bättre än tidigare. Idag finns säkerhetsrevisioner och penetrationstester hos R4s företag, men de behöver processkarta samt kommer att radera besökarnas data automatiskt. R5 tyckte att små till medelstora företag har säkerhet på plats men tänkte inte så mycket på integritet. Enligt R6:s berättelse skiljer det mellan organisatoriska förändringar såsom samtycken med kunder, då själva bilderna är personuppgifter som inte direkt påverkas av förändringar. Skillnad finns efter att en bild är tagen, när kunden vill ta bort sin bild exempelvis. Därför blir det enligt R6 en förändring i back-end systemet vilket måste synkas i backupperna. Dock har alla bolag det så, inte bara säkerhetsbolag. ”Privacy by design” - måste tas in i utvecklingsprocessen mycket tidigare än innan, därför blir det en stor förändring i utvecklingsprocesser enligt respondenten. Det är en stor kedja som måste tänka på säkerheten enligt respondentens berättelse. Dekonfiguration måste finnas så enheten inte skickar data automatiskt om kunden inte vill det. Anonymisering av datan kan göras för att koppla bort kopplingen mellan individen och datan men man måste förklara för kunden vad som ska hända och varför.

4.3.5 Implementering och uppföljning

R1 uttryckte att process metodiken kommer att säkerhetsställa resultatet hos sitt företag. R3 berättade att företaget köper in industri-ledande system för att hålla koll på olika aspekter, vilket möjligtvis kommer att förverkligas i en awareness program. R4:s företag använder sig av bland annat revision, genomför penetrationstest 1 gång per år med externa aktörer, samt är företaget försedd med egna verktyg till interna penetrationstester vilka utförs 5 gånger per år samtidigt som företaget skickar ut uppdateringar. Företaget ligger enligt R4 “dåligt till” när det kommer till att producera dokument om exempelvis processkartläggning, vilket enligt

respondenten bör förbättras. R6 påpekade att företag måste fortsätta arbeta med GDPR kontinuerligt, eftersom förordningen inte är en engångshändelse:

“Om de har en ny funktionalitet så måste de göra en konsekvensbedömning, “data protection impact assessment”, och riskarbete, samt se över samtycken, att de stämmer överens med nya funktioner. Det krävs kontinuerligt förändringsarbete av data protection officer, ”dataskyddsombud”.” (R6)

5. ANALYS

I detta kapitel sker analysen av det inhämtade empirin i jämförelse med den teoretiska referensramen som presenterades under kapitel 3. Syftet är att förbereda det insamlade materialet till diskussion genom att förstå intervjumaterialet genom att koppla respondenternas svar till relevant teori. Kapiteln är uppdelade i tre underkapitel för att tydliggöra analysens koppling till forskningsfrågorna på ett systematiskt och tydligt sätt för läsaren. Delkapitel 5.1 stödjer förståelsen för delfråga 1, 5.2 för delfråga 2 och 5.3 ger förståelse för delfråga 3.

5.1 Informationssäkerhet och integritet före GDPR

Både O'Brien (2016) och respondenterna menar att om företagen förvarar data så behöver de automatiskt följa GDPR-kraven. I empirin framkom det att företagen vars anställda intervjuades förvarade data, åtminstone till viss del, vilket gör att de måste uppfylla kraven. Typen av och därför även värdet på datan som samlas in skiljde sig mellan företagen och enligt Sherwood et al (2005) bör därför nivån på säkerheten anpassas till detta. En av respondenterna berättade om att företaget personen arbetar på höll på att införa en utvärdering av olika data kategorier. Det är dock oklart huruvida resterande företag utför någon form av sådan utvärdering men eftersom det rör sig om bilder från kameror så kan ett antagande göras om att datan är av hög känslighetsgrad.

Sherwood et al (2005, 29) antagande om att tillämpning av en checklista misslyckas har inte bevisats men inte heller motbevisats i empirin, eftersom dokumenten hölls hemliga på grund av stora mängder tekniska detaljer. Därför går det inte att jämföra kraven som används i praktiken med teorin inom området. Det som dock framkom i empirin var att användningen av kravspecifikationer skiljde sig mellan företag. Några av respondenterna berättade att företagen använder någon form av kravspecifikationer eller annan dokumentation som stöd i utvecklingen. En av respondenterna berättade om att väldigt detaljerade kravspecifikationer används, medan en annan förklarade att företag försöker gå ifrån att använda kravspecifikationer, eftersom det inte leder till bästa resultat vilket kan då kopplas till Sherwood et al (2005, 29) teori.

Carroll et al (2012) teori om att det är svårt att kvantifiera hur säkert ett system eller en organisation är bekräftades i empirin, eftersom resultatet av intervjuerna visade att respondenterna fastän de arbetar hos företag som antingen utvecklar eller förmedlar säkerhetslösningar upplever att företagen är "ganska rustade" när det gäller informationssäkerhet. Empirin visade att alla av de undersökta företagen använder sig av flera och omfattande säkerhetslösningar men respondenterna själva har svårigheter med att avgöra och klassificera var systemen eller företaget ligger inom säkerhet. Ena respondentens berättelse om att "det är svårt att bestämma hur mycket är tillräcklig säkerhet" (R6) bekräftar Carroll et al (2012) teori ytterligare. Intervju resultatet visar även på att företag som är involverade i utvecklingen av säkerhetssystem med smarta kameror har en hög säkerhet och uppnådde flera av GDPR-kraven redan innan regelverket infördes. Detta syns i att vissa av respondenterna själva uttryckte att det inte var "särskilt farligt med GDPR", men att det fortfarande var en belastning. Enligt datan insamlad från intervjuer samlas information in vid användning, men detta med syftet att möjliggöra användningen av tjänsten och respondenternas berättelse om att data inte används till andra syften, visar tydligt på att detta GDPR krav redan är uppfyllt.

Enligt teori bör ett företag beakta både ett helhetsperspektiv och detaljnivå, för att uppnå en hög säkerhet. Empirin tyder på att företagen betraktar informationssäkerhet utifrån ett holistiskt perspektiv (O'Brien, 2016; Sherwood et al, 2005), vilket syns i bland annat att det upprättas kontrakt med underleverantörer, det säkerställs en fysisk säkerhet och de flesta av studieobjekten håller på att utbilda anställda i varför GDPR är viktigt. Att betrakta säkerhet utifrån ett helhetsperspektiv kommer behöva uppfyllas kontinuerligt, eftersom GDPR påverkar alla delar av en organisation, inte bara IT avdelningen. Det har inte kommit fram ett svar om hur studieobjekten kommer att åstadkomma helhetsperspektivet i empirin men det görs ett antagande om att företagen kommer fortsätta ha en grupp ansvarig för GDPR i syfte att tillhandahålla ett holistiskt perspektiv. En sådan grupp möjliggör även integrering av arbetet med säkerhet och integritet, vilket enligt O'Brien (2016) inte ska ske i separata avdelningar. Det ger dessutom en helhetssyn på säkerhet och gör att den inte blir isolerad från affärsprocesser, vilket Sherwood et al (2005) menar händer om säkerhet adderas efter implementering. Hans påstående får inte stöd i empirin i detta fallet, eftersom hos vissa företag innehåller kravspecifikationer bland annat detaljer kring säkerhet, vilket tyder på att säkerhet betraktades innan implementeringen redan före GDPR. De företagen som beaktar säkerhet innan implementeringens tillfälle arbetar redan utifrån Privacy by Design enligt respondenterna.

Empirin visar även på att företagen har en detaljerad intelligens (O'Brien, 2016) genom att exempelvis logga varje händelse i systemet, införa datakategorisering, dokumentera. Detta innebär att studieobjekten ligger ovanför grundlösningen och skapar bevis om Privacy by Design. Ett sådant tillvägagångssätt ligger även i linje med *The evolution of information assurance* (2002), då säkerhetsfunktionalitet distribueras mellan enskilda enheter.

Både teori och empiri har visat på att ISO 27001 certifiering kan vara relevant för att visa på att ett företag uppfyller GDPR-kraven och samtidigt uppehålla legitimitet (Jacobsen och Thorsvik, 2008). Alla företagen vars anställda intervjuades har redan eller höll på att implementera ISO 27001, vilket visar ytterligare på deras höga nivå av säkerhet hos de företagen som redan implementerat ISO 27001 och en medveten strategi för att upprätthålla legitimitet hos de företag som just nu implementerar det.

5.2 Anställdas inställning till och förståelse för GDPR

Angående motivation skrev Jacobsen och Thorsvik (2008, 294) att avsaknad av information kan vara en orsak till bristande motivation och samtidigt kan leda till frustration bland medarbetare, vilket delvis kan kopplas till empirin eftersom ena respondenten hävdade att det var en dålig informering till företag om att det ens kommer en ny förordning. Bristande motivation har dock inte påvisats i empirin till följd av svag informering vilket betyder att Jacobsen och Thorsviks (2008, 294) teori har inte fått stöd i empirin.

Colesky et al (2016) påstående om att GDPR formulerar bara mål och att det fortfarande existerar oprecist språk i GDPR överensstämmer med empirin, eftersom fyra av sex respondenter menade att GDPR inte är tydligt beskriven. Enligt respondenterna beror deras uppfattning på den svåra tolkningen av GDPR och sättet det är beskrivet på är "luddigt", vilket då kan kopplas till Colesky et als (2016) mening om att lagstiftningar inte brukar överlämna tydliga krav. Otydligheten förklaras av två respondenter genom att det är den svåra tolkningen av rollerna som datakontrollant och den svåra tolkningen av vad som räknas som känslig information och persondata, vilka gör det svårt att veta hur implementeringen av GDPR praktiskt skall utföras. Enligt ena respondenten vore det gynnsamt om GDPR innehöll konkreta exempel. Bara R6 tyckte att GDPR är tydlig, men tillägger att enligt sin erfarenhet

bedömer oftast företag GDPR som oklar. Samtidigt så finns det organisationer som skriver artiklar som ska förtydliga GDPR med praktiska exempel. En sådan organisation är Article 29 som berördes i empirin. Där spekulerar en av respondenterna att detta kommer bli det officiella ramverket för GDPR. Respondenten tillägger att det kommer för sent och därför är det rimligt att företagen upplever att GDPR är otydlig. Ena respondentens tanke om att det kanske kommer en uppdatering av GDPR då det behövs kompletterande material för att använda den, styrker ytterligare GDPR:s otydlighet och härmed Colesky et als (2016) teori i det undersökta sammanhanget.

Att förordningar har stor betydelse och påverkanskraft på företag påvisades i empirin, eftersom enligt ena respondenten kan GDPR ha påverkan på bland annat tillverkningskostnader, vilket i sin tur kan innebära att det blir dyrare för konsumenten då säkerhet enligt personen är dyrt, eftersom det innebär speciell kunskap. Enligt ena respondenten kan det därför förekomma att företag köper in mindre säker hårdvara. Att det förekom i empirin att säkerhet är dyrt enligt ena respondenten, kan förklaras med Junwoo et als (2017) antagande om att företagets kostnader kan tre- eller fyrdubblas i följd av GDPR. Det har dock inte tydligt bevisats i empirin, vilket kan bero på att GDPR inte har trätt i kraft än vid undersökningens tidpunkt, vilket enligt tre respondenters berättelse beror på att det är svårt att bedöma konsekvenserna av GDPR innan den träder i kraft.

Tre av sex respondenter tyckte att implementeringen av GDPR ibland innebär en begränsning vilket enligt två respondenter beror på att GDPR begränsar vad företaget vill göra utöver dess otydlighet. Samtidigt visar resultatet av intervjuerna att GDPR även innebär en möjlighet för företag, eftersom enligt två respondenter kan företag bland annat bygga sitt varumärke genom att synliggöra att de tänker på sina kunder och visa på att de gör det bättre än sina konkurrenter. Uttalandet kan ha sin grund i Jacobsen och Thorsviks (2008, 233, 244) teori om att de företag som inte följer lagar och bestämmelser kan resultera i ett försvagat rykte och legitimitetsproblem. Vidare beskriver dock inte Jacobsen och Thorsvik (2008, 233, 244) om företag som följer lagar och bestämmelser höjer sin legitimitet gentemot sina intressenter, eller om det kanske bara är ett minimum krav. Detta resultat kan utöver Jacobsen och Thorsviks (2008, 233, 244) teori underbyggas med Junwoo et als (2017) studie som visade att oroligheten bland företag på grund av GDPR resulterat i att mer än hälften av de tillfrågade IoT företagen överväger att byta sina affärsstrategier. Jacobsen och Thorsvik (2008, 233, 244) tillägger att misslyckande att förhålla sig till lagarna kan resultera i bestraffning, vilket Zerlang (2017) förstärker genom sitt påstående om att företagen själva bestämmer om de vill dra fördel av GDPR eller istället väljer att betala böter. Intressant är att enligt ena respondenten förstår vissa företag inte att GDPR inte bara är en tillfällig händelse, men en kontinuerlig omständighet.

Sandholm (2012, 298) menar att förändringar kan upplevas som ett hot, vilket kan medföra motstånd genom bland annat att människor låser sig vid sina egna tolkningar. Sandholms (2012, 298) påstående visas tydligt i resultatet av intervjuerna, eftersom den ena respondenten tyckte att det även går att argumentera för att kunden är kontrollant och en annan respondent som berättade att det är otydligt om det behövs en DPO i företaget eller inte. En tredje respondent som tyckte att "all initiativ till att bli kompatibel blir bara större och svårare" kan också kopplas till Sandholms (2012, 298) teori om egna tolkningar. Företagen måste däremot ha tolkat den otydliga beskrivningen på något sätt för att kunna implementera GDPR, vilket då blir ekvivalent med en egen tolkning som går i linje med Sandholms (2012, 298) teori. Tydligt motstånd mot förändringen som GDPR innebär visade sig dock inte i empirin, vilket antingen är en underförstådd känsla eller något som respondenterna avsiktligt har valt att inte berätta om, förutom en respondent vems företag beaktar GDPR som ett hot. Sandholms

(2012) teori om att undvika motstånd genom att erbjuda deltagande har delvis bevisats i empirin, eftersom flera av de tillfrågade företagen både har en juridisk avdelning som kan rådfrågas och en GDPR grupp som arbetar med att implementera förändringarna och samtidigt involverar flera avdelningar och medarbetare i processen. Ena respondenten uttryckte dock att det förekommer brister kring återkoppling från GDPR gruppen.

5.3 Implementation av förändringar i samband med GDPR

Resultatet av intervjuerna har visat att flera av de företagen som respondenterna jobbar hos redan har uppfyllt många av GDPR-kraven, då som det beskrivits under 5.1 använder flera av företagen inte data till något annat. O`Briens (2016) teori om att företagens integritetsmognad är betydelsefull när det gäller uppfyllelse av GDPR villkor påvisades i empirin genom att alla respondenter förutom experterna arbetar hos företag som enligt respondenternas egen beskrivning redan arbetar utifrån en hög integritetsfilosofi. Zerlangs (2017) påstående om att generellt blir företag tvungna att öka säkerheten i sin data har inte fått stöd men inte heller motbevisats i empirin, eftersom studieobjekten redan innan har en hög säkerhetsfilosofi enligt respondenternas berättelse. Ena respondentens åsikt om att de största förändringarna sker organisatoriskt och inte tekniskt efter att en bild är tagen förstärker studiens relevans. En annan respondents berättelse om att de största förändringar de behöver införa är att dokumentera exempelvis processkartläggning bättre påvisar inte heller Zerlangs (2017) teori då det belyser förändring i dokumentation och inte ett behov av högre säkerhet.

I empirin framkom det att i varje studieobjekt arbetar ett specifikt team med implementeringen av GDPR genom att bland annat tolka, driva och implementera förändringarna i alla system. Ena respondentens berättelse om att GDPR gruppen intervjuade alla avdelningar om hur de arbetar och en annans beskrivning om att även juridisk expertis är involverad påvisar Longs (2017) teori om att GDPR innebär en komplex förändring och har en signifikant påverkan på varje del i organisationen. Ena respondentens påstående om att det sker mycket förändringar bakom kulisserna på grund av GDPR påvisar ytterligare Longs (2017) teori.

Ena respondentens berättelse om att "Privacy by design" förändrar utvecklingsprocesser rejält bekräftar O`Briens (2016) påstående om att inkluderingen av integritet i företagens processer och aktiviteter är nödvändigt för att lyckas överensstamma GDPR:s förutsättningar. Vidare anser O`Brien (2016) att de företag som beaktar "Privacy by design" utför en proaktiv riskhantering, vilket som tidigare beskrivits (5.1 Informationssäkerhet och integritet före GDPR) arbetar flera av de undersökta företagen utifrån. Att empirin visade att implementeringen och uppföljningen av GDPR i framtiden kommer att ske genom kontinuerlig revision, penetrationstester, uppdateringar, konsekvensbedömning, riskarbete, inkludering av integritet genom design (privacy by design) och att uppdatera samtycken vid nya funktionaliteter då det krävs ett kontinuerlig säkerhetsarbete tyder på ett proaktivt säkerhetsarbete (Zerlang, 2017), vilket enligt Zerlang (2017) förenklar implementeringen av GDPR.

Att resultatet av intervjuerna visade att de tillfrågade företagen skärper sina avtal mot sina leverantörer bevisar IT Governance Teamets (2016) påstående om att kontraktskrivning med andra aktörer minskar företagens sårbarhet eftersom det styrker att data behandlas på ett säkert sätt. Komplexiteten med GDPR i en IoT kontext (Long, 2017; Lindquist, 2017) bekräftades ytterligare i empirin genom att flera respondenter upplever en svårighet med att upprätta massvis med avtal och därför tyckte ena respondenten att ett standardavtal från EU skulle bli uppskattad. Svårigheter med kontraktskrivningen som empirin visade kan även

förklaras med Jacobsen och Thorsviks (2008, 431) teori om att organisationsförändringar innebär nya förhållanden till externa parter. Lindqvists (2017) antagande om att en kontinuerlig kontroll av kontrakten mellan IoT intressenterna är nödvändigt har inte påvisats men inte heller motbevisats i empirin. Däremot är en intressant upptäckt att enligt ena respondenten kan överskjutning av ansvar till den som gör sluttjänsten förekomma.

Niese et als (2016) antagande om att erbjuda informerade samtycken till användarna är komplext och är en utmaning i en IoT kontext har fått stöd i empirin, eftersom flera respondenter uttryckte att det är svårt att visa integritetsmeddelanden som skall samlas in strax innan datainsamling, eftersom produkterna inte har någon skärm. En annan respondentens berättelse om att samtycken måste vara specifika inför alla nya funktionaliteter och att samtycken inte får bli stoppande får härmed stöd i Niese et als (2016) teori. Niese et als (2016) påstående om att det enda sättet att behandla data på ett rättvist sätt är genom att samla in samtycken från användarna har dock inte bevisats i empirin, eftersom flera av de tillfrågade företagen använder sig av anonymisering av data eller motiverar att användningen av data behövs för att kunna leverera tjänsten enligt överenskommelse med användare.

Thorsviks (2008, 426) teori om att en planerad förändring kräver bland annat säker kunskap och en lyckad implementering synliggjordes i empirin genom att vissa respondenter berättade att företagen använder sig av leveransstöd i form av GDPR-konsulter. Respondenternas berättelse om rådfrågning och feedback från GDPR-gruppen och den juridiska avdelningen (5.2) kan förutom Sandholms (2012) teori analyseras med hjälp av Sims (2002) påstående om att involvering av medarbetare har ett positivt inflytande på implementeringens framgång. Det innebär att de företagen som involverar sina medarbetare under implementeringen av GDPR vilket är en förändring i sig, har en större chans att lyckas med implementeringen samtidigt som att motstånd mot förändring förebyggs.

Zerlang's (2017) påstående om att det blir en utmaning att bryta ned siloerna i processen under implementeringen har delvis bevisats i empirin då ena respondenten tyckte att samarbetet med de medarbetare som sitter nära fysiskt är bättre, eftersom vid fysiskt avstånd är kommunikationen svårare. Det visar sig att så fort det förekommer fysiskt avstånd försvåras då samarbetet eftersom avdelningarna sitter i sina egna siloer med avstånd från varandra. Om vi då kopplar in Longs (2017) teori om GDPR:s komplexitet och att det påverkar alla avdelningar i organisationen samtidigt som vi beaktar O'Briens (2016) och Sherwood et als (2005) teori om att företag bör beakta både ett helhets- och detaljperspektiv (5.1) får vi fram att företag som inte hanterar GDPR:s komplexitet framgångsrikt vid implementeringen även vid fysiskt avstånd minskar utsikten till en lyckad implementering. Ena respondentens berättelse om att företaget för tillfället skapar en utvecklingsmodell eftersom alla behöver en viss förståelse tyder på företagets goda insikt i den komplexa förändringen som GDPR innebär. En andra respondent som talade om den knappa feedbacken från GDPR-gruppen, att personen inte vet när återkoppling av resultatet kommer att ske och ansåg att eftersom avdelningen inte förvarade någon data så behöver den inte göra något (4.4) visar däremot på att företaget eventuellt inte har brutit ned silorna och eventuellt inte har både ett helhets- och detaljperspektiv vilket kan försvåra en lyckad implementering enligt Zerlang's (2017), Longs (2017) och Sherwoods et als (2005) teori.

Flera respondenter uttryckte att det är en svårighet och utmaning att både ta bort användarnas data inom 72 timmar och att informera användarna om sin datas livscykel, eftersom företagen då måste ha kännedom och medvetenhet om datans hela livscykel. Det bekräftas av Zerlang's (2017) teori om att implementeringen kräver en omfattande granskning av bland annat företagets egna system och processer. Ena respondentens åsikt om att varumärket och

aktiekursen påverkas negativt om en dataläcka inträffar och en annan respondentens berättelse om att de använder sig både av en vulnerability board och PR-människor vid en sådan händelse, kan kopplas till Borglund et als (2012) teori om att förtroendet påverkas negativt om företag inte följer riktlinjer och inte heller visar sin kompetens. Samtidigt uttryckte ena respondenten oro om hur det skall kunna följas upp att sekundär användning av data inte sker, eftersom företag kan dölja att någonting hade läckt genom att påstå att data har läckt säkert.

Tankards (2016) påstående om att anonymisering är ett lämpligt skydd så länge det inte går att koppla data till en specifik individ har delvis bevisats i empirin, eftersom ena respondenten tyckte att anonymisering kanske inte är tillräckligt och vilket enligt en annan respondent är svårt att lösa praktiskt och därför kan det vara nödvändigt att implementera extra funktioner men tillade att: "man behöver hitta ny lösning för varje scenario".

Borglund et als (2012) teori om att företag kan vinna förtroende genom bland annat att certifiera sig och följa riktlinjer, tydligt bevisades i empirin genom att flera respondenter nämnde att de företagen de arbetar hos antingen planerar att införa eller redan har implementerat ISO 27001. Utöver ISO 27001 certifieringen inför vissa av de företag som undersöktes även en säker utvecklingsmodell och tar fram eget best practise med data inventory. GDPR ingår som ett hot i hot-modelleringen enligt ena respondenten, vilket kommer att bekantgöras i efterhand inom organisationen.

Zerlangs (2017) teori om att DPO:n presenterar att företag erkänner data som en viktig komponent till företagets framgång och att DPO:n förses med en holistisk översikt över data som företag behandlar, kan enligt resultatet av intervjuer vara problematiskt. Ena respondentens påstående om att de företag som inte har resurser till att anställa säkerhetsexperter till rollen som DPO, kan utnämna en utvecklare till DPO vilket enligt ena respondenten kan utgöra ett problem eftersom även erfarna utvecklare inte vet hur de ska hantera GDPR. Zerlangs (2017) teori om att det är DPO:n som förser företag med en holistisk översikt över datan bevisades i empirin, då en av experterna menar att DPO:n är den ansvarige och den man ska kontakta vid frågor (4.4, Vem har ansvaret?).

Att GDPR ämnet visas i ledningsagendan (O'Brien, 2016) bevisades i empirin, eftersom alla av de undersökta företagen avsatt resurser för uppfyllelse av GDPR-villkor. Att företagsledningen genomgått specifik utbildning inom GDPR (O'Brien, 2016) har dock inte fått stöd men inte heller motsattes i empirin eftersom inga respondenter berörde ämnet.

6. DISKUSSION

Nedan diskuteras analysens utfall. Underkategori 1 knyter an till forskningsfråga 1, underkategori 2 till forskningsfråga 2 och underkategori 3 till forskningsfråga 3. För att underlätta för läsaren presenteras forskningsfrågorna i kursiv under varje delkapitel. Syftet med diskussionen är att reflektera över studiens analys, att besvara forskningsfrågorna utifrån studiens syfte och att förbereda materialet till slutsatsen.

6.1 Informationssäkerhet och integritet före GDPR

Delfråga 1: Hur ser företagens tillstånd och arbete med säkerhet och dataintegritet ut före GDPR vid utveckling och drift av smarta kameror?

Hypotesen var att företag som är involverade i utveckling av säkerhetslösningar redan uppfyller mest av GDPR-kraven men det finns mindre förhållanden som behöver anpassas, samt att det förekommer utrymme till förbättring av företagens dataintegritets-mekanismer. Studieobjekten har enligt analysen redan innan implementeringen av GDPR en tillräckligt hög nivå av säkerhet, både överlag och när det gäller detaljer men som det nämndes i analysen så är det komplicerad att avgöra ett företags säkerhetsnivå. Att anställda inte själva kan avgöra nivån på t.ex. en skala betyder inte att företaget inte är skickligt eller saknar några viktiga delar. Det visar bara hur komplicerad bedömningen är. Det kan dock emellertid vara svårt att veta att något saknas och då upplevs säkerheten som hög, även om den inte är det. För att göra en mer objektiv bedömning av säkerhetsnivån kan arbetssättet och effekter av det undersökas. I analysen har arbetssättet inom flera områden visat sig ligga i linje med forskning inom området och därför bedöms som tillfredsställande. Men insatserna kan inte utvärderas utan att titta på resultaten. En djupgående undersökning av produkternas säkerhet har legat utanför uppsatsens ramar men vid intervjuer har det ställts frågor om upptäckta buggar och dataläckor, vilka hade kunnat vara ett tecken på låg säkerhet. Enligt respondenterna uppkommer det alltid något form av fel i produkterna, men det mesta brukar fångas upp under utvecklings-, samt testningsprocessen och det har inte uppkommit några allvarliga felaktigheter som inte kunde åtgärdas och uppdateras. Baserat på utvecklingsprocessen och det överlag goda resultatet anses därför det ursprungliga antagandet ha bekräftats. Det går dock även att argumentera för att säkerhetsnivån av produkterna endast bedöms av anställda och därför inte är objektivt, vilket då skulle innebära att insatsen, det vill säga utvecklingsprocessen inte lyckas säkerställa produkternas säkerhet. Argumentet kan motbevisas med att studieobjekten har en ISO 27001 certifiering, vilket är ett tydligt och pålitligt bevis för att hypotesen stämmer. Detta bör dock ändå undersökas vidare och en mer djupgående utvärdering av produkten bör göras.

Dessutom måste det poängteras att säkerhet och integritet inte är samma sak. Något som inte riktigt behandlas i arbetet är frågan om att hur stor utsträckning båda delar utvärderas till vid testning. Det kan till exempel förekomma att om säkerheten är tillräckligt hög, så kommer testarna aldrig fram till att testa integriteten. Då kan kanske dataintegritet kollas vid penetrationstest, där testpersoner låtsas som att säkerheten har tacklats, även om den egentligen är hög i syftet att testa integriteten.

Den varierande användningen av kravspecifikationer kan jämföras med en teori inom ledarskap om ledarens positiva versus negativa syn på anställda. Det är intressant ifall denna teori kan utvidgas med kravspecifikationer och policier (eller mål och visioner). Kravspecifikationer kan vara som en "piska" för anställda som får dem att känna att ledaren har en negativ syn och inte litar på deras kunskaper och vågar därför inte överlämna dem

ansvar. Men om företaget istället använder sig av en policy så kan det möjligtvis motivera människor till att ta mer ansvar och jobba mer för att skapa en bra produkt. Samtidigt om företagen bara har en vision, då kan eventuellt viktiga detaljer eller komponenter till säkerhet och integritet missas. Därför kan det vara intressant att undersöka om en blandning av både kravspecifikation och policy skulle resultera i en högre säkerhet och mer motiverade medarbetare än användning av endast policy eller kravspecifikation.

6.2 Anställdas inställning till och förståelse för GDPR

Delfråga 2: Vilken inställning och förståelse har anställda för GDPR vid utveckling och drift av smarta kameror?

Som det tidigare beskrivits i analysen anser de flesta av respondenterna att företagen de arbetar hos har en hög integritetsmognad och kan därför enligt O`Briens (2016) teori uppfylla GDPR-kraven väl. Intressant, om det kan finnas andra aspekter förutom ett företags integritetsmognad för att tillämpa GDPR:s villkor i hög grad i en organisation, vilket har fallit utanför studiens ramar, men svaret på frågan skulle medföra ytterligare stöd för andra företag utanför säkerhetsområdet som både enligt vår antagning och vissa respondenternas åsikt har svårare förutsättningar att tillgodose GDPR-kraven.

Colesky et als (2016) teori om oprecist språk innebär då som beskrivet i analysen en avsaknad av information vilket enligt Jacobsen och Thorsvik (2008, 294) kan leda till bristande motivation. Båda teorierna bevisades i empirin enligt ovan, vilket kan betyda att det otydliga språket i GDPR resulterar i att företag upplever förordningen som en begränsning och som kan ha lett till en bristande motivation. Teorier om att en upplevd begränsning skulle kunna minska motivationen hittades dock inte. Att motivationen hos företagen är minskade har vi dock inte fått svar på från empirin, men kan vara ett resultat som antingen respondenterna inte medvetet tänker på och känner eller medvetet valde att inte prata om.

Intressant, att endast enligt R6 är GDPR tydligt beskriven och enligt personen uppfattar de flesta företagen personen hjälpte till tyckte att förordningen är otydligt. I och med att R6 har en konsultroll, påverkas personen inte av förändringen på samma sätt som respektive företagens medarbetare. Medarbetarna är däremot direkt involverade i GDPR och upplever det som otydligt, vilket kan betyda frustration mot förändringen som det står i Colesky et als (2016) teori. Experten är konsult, inhyrd av företagen och känner sig inte frustrerad antingen på grund av sin expertis eller att personen inte blir påverkad av GDPR inom företaget i längden.

Otydligheten i GDPR som bekräftades i resultatet och som är analyserad under punkt 5.2 kan ha medfört oro bland företagen. Flera respondenter menade att det finns en risk med att de missar någonting, eftersom det är en utmaning att tolka förordningen rätt. Det påverkar dock inte bedömningen om företagen redan är kompetenta inom säkerhet och integritet, men resultatet tyder på en brist hos GDPR:s tydlighet snarare än brist hos företagen.

Ena respondentens berättelse om brister kring återkoppling från GDPR-gruppen påvisades i analysen att företaget riskerar att själv bygga motstånd bland sina medarbetare mot förändringen genom otillräcklig återkoppling. Ökad involvering och deltagande av anställda genom hela organisationen skulle minska risken för motstånd. Eftersom motstånd försvårar implementering och acceptans, är det nödvändigt att involvera medarbetare på alla plan inom organisationen.

Jacobsen och Thorsvik (2008, 233, 244) beskriver dock inte tydligt att företag som följer lagar förstärker sin legitimitet och rykte. Det kan bero på att uppfyllelse av GDPR-kraven blir ett måste för alla företag utan undantag och om dess krav inte uppfylls så lämnar kunderna. På så sätt blir säkerhet en slags hygienfaktor som är kritisk för kunderna men som inte motiverar de till att köpa just denna produkt.

6.3 Implementation av förändringar i samband med GDPR

Delfråga 3: Vilka förändringar kommer företag behöva implementera för att uppnå GDPR-kraven vid utveckling och drift av smarta kameror?

Oron som analysen visade om att säkerställa att sekundär användning av data ej ägt rum (eftersom företag kan hävda att data har läckt säkert), kan innebära att GDPR:s rekommendationer inte är tillräckliga eller kan kringgås.

Att företagen använder sig av GDPR-konsulter kan tyda på företagets förståelse för att det krävs säker kunskap för en planerad förändring och till en lyckad implementering, vilket samtidigt kan visa på företagets mognad.

Implementationen av ISO 27001 som är erkänd av GDPR leder inte bara till förtroende från kunderna, men samtidigt genom certifieringen skulle företagen kunna uppvisa sitt ansvarstagande vilket i sin tur kan ha en positiv påverkan på organisationens varumärke.

Intressant diskussion om resultatet är Borglund et al (2012) teori om hur företag vinner förtroende. Vid en eventuell dataläcka är företag enligt GDPR skyldiga att berätta om att en läcka har inträffat, vilket är just transparens av relevant information som Borglund et al (2012) menar är ett av fyra sätt till att vinna förtroende. Men resultatet visade att det finns en oro kring den negativa påverkan på varumärket vid en eventuell dataläcka. Betyder det att företag genom sin transparens vid en dataläcka höjer intressenternas förtroende för företaget, vilket enligt Borglund et al (2012) sker, eller sänks intressenternas förtroende? Eller att just för att ens en dataläcka hade kunnat inträffa visar på företagets inkompetens, vilket då enligt Borglund et al (2012) sänker förtroendet för företaget? Hur ser förtroendet ut för ett företag som är transparent om en läcka inträffar? Hur påverkar det varumärket?

Det finns en oro från de undersökta företagens sida i samband med att berätta om dataläckor som har skett, eftersom det kan uppfattas som tecken på inkompetens och skulle kunna leda till negativa effekter i form av förlust av kunder eller investerare. Åt andra sidan säger Borglund et al (2012) teori att företag kan vinna kundernas förtroende om de är transparenta, följer riktlinjer och visar välvilja mot andra. Att inte undagömma att en dataläcka har skett och istället öppet informera om det hade kunnat ses som ett tecken på dessa. Det kan därför vara intressant att fördjupa sig i vilka effekter publicering av negativ information har på kundernas uppfattning om berörda företag.

Insamling av samtycken visade sig vara en utmaning i en IoT kontext enligt analysen, vilket nämdes är det enda rättvisa sättet att behandla användarnas data på. Att de undersökta företagen använder sig av anonymisering eller motiverar användningen av data istället för att samla in samtycken kan bero på att GDPR inte är anpassad till en IoT kontext och därför kan företag bli tvungna att använda sig av anonymisering eller motivering till användning istället för att samla in samtycken från kunderna. Detta tillvägagångssätt kan påverka förtroendet för företaget i en negativ riktning, eftersom de användare som inte har en förståelse för vilka utmaningar det innebär att samla in samtycken genom IoT kameror kan lägga märke till att andra företag som behandlar sin data utanför IoT området däremot möjligen använder sig av

samtycken. Det kan innebära problematik för företag i en IoT kontext vilket kan vara av vikt att beakta och finna lösning på.

Zerlans (2017) teori om hur betydelsefull rollen som en DPO presenterar skulle behöva utökas med ett krav om att DPO:n verkligen lever upp till att förse företaget med en holistisk översikt över all data som behandlas för att kunna kringgå problematiken med resursbrister.

Det kan vara relevant att diskutera hur arbetet med GDPR kommer att se ut i framtiden. I analysen undersöktes nuläget, innan förordningen har trätt i kraft men som en av respondenterna påpekade så kräver GDPR ett kontinuerligt arbete med integritetsfrågor. Ett antagande om att företagen kommer fortsätta jobba på samma sätt men det är osäkert om detta stämmer. Det verkar finnas olika lösningar. Om GDPR-gruppen under implementeringen bestod av externa konsulter måste konsulterna anlitas vidare, alternativt måste några av de anställda utses till DPO rollen, vilket då kräver resurser, för att den anställda ska kunna få omfattande utbildning. Om GDPR-gruppen bestod av utvecklare som redan har fått utbildning blir det enklare, eftersom de bara kan fortsätta jobba på samma sätt, eftersom de redan besitter erfarenhet om företagets processer och vilken data de behandlar. Det går dock inte att utifrån materialet för uppsatsen bedöma vilket av tillvägagångssätten ger bästa resultat.

7. SLUTSATS

Även om GDPR inte är anpassat till IoT så måste företaget ändå anpassa sig mot förordningen. Hypotesen bekräftades under studien, eftersom alla de undersökta företagen redan innan GDPR har en hög integritetsmognad och säkerhetstänkande utifrån respondenternas berättelse vilket analyserades med befintlig teori inom området, men det förekom även flera aspekter som företagen behöver förändra och anpassa för att överensstämma med GDPR-kraven. Studiens syfte var att hitta och presentera huvudsakliga förhållanden som behöver förändras i utveckling och drift av smarta kameror (Delfråga 3) i jämförelse med tillståndet innan GDPR (Delfråga 1) samt att överlämna förslag på förbättringsområden till studiens målgrupp som är företag av den typen som arbetet undersöker, vilket har uppnåtts.

Forskningsfrågan var följande: **“Vilka förändringar behöver företag implementera för att uppfylla GDPR-kraven jämfört med tillståndet innan samt vilken inställning har anställda till förändringen i utveckling och drift av smarta kameror för att implementeringen skall bli lyckad?”** Studien visade på följande fem huvudsakliga förändringar som behöver införas hos studieobjekten i samband med GDPR:

1. Finna lösning på insamling av informerade samtycken trots problematiken med att IoT kameror har ingen skärm, eftersom det enligt teorin visade sig vara den mest rättvisa sättet att samla in personuppgifter på. Utifrån intervjuerna väljer studieobjekten däremot att antingen motivera sin datainsamling, vilket i sin tur kan leda till minskad förtroende från kunderna, eller väljer att använda sig av anonymisering vilket resulterar i att data blir mindre värd. Samtycken får samtidigt inte bli stoppande, vilket bör möjliggöras tekniskt.
2. Företagens behandling av personuppgifter måste bli grundligt dokumenterad genom loggning, införelse av datakategorier och processkartor i syfte att skapa bevis om GDPR-kravens uppfyllelse.
3. Trots den hastiga teknologiska utvecklingen vilket resulterar i komplicerade relationer bland företag som leder i sin tur till mängder av diverse avtal, är företaget skyldig att skydda personuppgifter även utanför verksamhetens gränser. I syfte att säkerställa att företagens data är säker hos andra aktörer krävs det en kontinuerlig kontroll av kontrakt mellan IoT intressenter. Överskjutning av ansvar till företaget som utför sluttjänsten kan förekomma, vilket kräver uppmärksamhet.
4. Genomföra ändringar i backend systemet för att kunna fullborda när en kund begär ut all sin data eller vill att företaget tar bort sin data. Att göra det tekniskt möjligt är nödvändigt för företag.
5. Betrakta säkerhet i utvecklingsprocessen genom “Privacy by design” och ett helhetsperspektiv som utgår ifrån affärsprocesserna. Alla anställda bör dessutom ha förståelse för och kännedom till GDPR och dess konsekvenser.

I studien undersöktes företag som utvecklar och drifvar smarta kameror. Baserat på dessa identifierade förändringar kan strategier till uppfyllelse av GDPR framställas hos både studieobjekten, men även hos företag som utvecklar andra IoT produkter. Anledningen till att generaliseringen görs till IoT företag är att just produkten påverkas inte mycket av förändringar, däremot strategier, utvecklingsprocess, arbetssätt, inställning och dokumentation påverkas vilka är överförbara till andra IoT företag.

En viktig del av förändringarna är att de inte möts av motstånd (Delfråga 2) och inget motstånd har uppmärksammats hos anställda som intervjuades. Trots att deras förståelse för GDPR var bristande så verkade inställningen vara positiv. Nedbrytning av siloerna och involvering av medarbetare utifrån studien är en nyckelfaktor. Bortsett från att GDPR innebär en utmaning till företagen, medför det även möjligheter i form av varumärkesbyggande och konkurrenskraftighet.

Följande förbättringsmöjligheter upptäcktes under studien: policy är bättre än kravspecifikation för att det resulterar i högre nivå inom säkerhet och integritet med mer motiverade medarbetare, ISO 27001 certifieringen rekommenderas av GDPR vilket kan vara nyttigt för företag att använda sig av för att inte bara uppfylla GDPR-kraven, men att stärka företagets legitimitet. Om företaget lyckas bevisa att de tänker på sina kunders integritet och bevarar deras data har det en positiv påverkan på varumärket. Certifieringen kan även ställas som ett krav på leverantörerna för att säkerställa säkerheten och integriteten utanför organisationens ramar. Det är nödvändigt att alla medarbetare har kunskap om säkerhet och integritet inom organisationen och att det integreras genom hela utvecklingsprocessen, vilket även höjer medarbetarnas motivation.

Slutligen måste det påpekas att nästan allt material som hittades betonar att IoT området i samband med GDPR är komplext. När ett komplext område kombineras med kvalitativa metoder så blir det en mängd olika aspekter att betrakta och undersöka. Det kan därför upplevas att uppsatsen är väldigt bred och behandlar många områden. Det finns samtidigt inte en specifik aspekt som kommer göra att ett system är säkert, utan det finns ett stort antal olika delar av ett system som måste vara på en hög nivå. Säkerheten bör beaktas ur ett holistiskt perspektiv vilket resulterar i att helheten fungerar men även detaljer bör beaktas, såsom varje del av produkten måste ha säkra features. Studien behandlade varje aspekt som uppkommit under intervjuerna och litteraturgenomgången. Framtida aspekter är antaganden, eftersom ingen riktigt vet hur framtiden kommer att se ut, förrän GDPR har trätt i kraft och fått tydliga konsekvenser.

8. FORTSATT FORSKNING

Följande intressanta aspekter framkommit, men som har fallit utanför studiens syfte:

Enligt GDPR kan personuppgifter skickas till tredje länder, det vill säga länder som inte tillhör EU eller EES, endast om ett antal villkor uppfylls. Att undersöka hur GDPR-kraven kommer att säkerställas vid sådana överföringar har legat utanför studiens ramar men kan vara ett relevant område att forska vidare på.

Frederick Herzberg (1959) är känd för sin tvåfaktorsteori, enligt vilken det existerar en separat uppsättning faktorer som motiverar anställda till arbete och en annan uppsättning med hygienfaktorer, som uppfyllda kan leda till att anställda skulle vantrivas. Det har diskuterats om säkerhet hade kunnat vara en liknande faktor, utan vilken kunderna skulle sluta köpa och använda en produkt. Det bör därför undersökas vidare, vilka andra hygienfaktorer kunder behöver i en produkt, eller vilka lojalitet faktorer det kan finnas som gör att kunderna fortsätter att köpa och stannar kvar.

Att undersöka skillnader mellan ISO 27001 och 9001, som är en kvalitetscertifiering har inte varit målet med studien. Slutsatsen bevisade dock att ISO 27001 är en "morot". Kombinationen av de två ISO standarder hade kunnat resultera i en säkerhet med hög kvalitè och kundfokus. Därför borde kombination av ISO 27001 och 9001 utforskas.

9. REFERENSER

- Ashton, K. (2009, Juni 22). That 'Internet of Things' Thing. *RFID Journal*. Hämtad 2018-02-06 från <http://www.rfidjournal.com/articles/view?4986>.
- Backman, J. (2016). *Rapporter och uppsatser*. Studentlitteratur AB, Lund.
- Belbachir, A. N. (2010). *Smart Cameras. [electronic resource]*. Boston, MA : Springer-Verlag US, 2010.
- Borglund, T., De Geer, H. & Sweet, S. (2012). *CSR Corporate Social Responsibility - En guide till företagens ansvar*. Livonia Print, Riga.
- Bugeja, J., Jönsson, D., & Jacobsson, A. (2018). *An Investigation of Vulnerabilities in Smart Connected Cameras*. IEEE Proceedings of the 2nd IEEE PerCom International Workshop on Pervasive Smart Living Spaces, 2018.
- Bugeja, J., Jacobsson, A. & Davidsson, P. (2017). *An Analysis of Malicious Threat Agents for the Smart Connected Home*. Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference. Doi: 10.1109/PERCOMW.2017.7917623.
- Carroll, T. E., Manz, D., Edgar, T., Greitzer, F. L. (2012). Realizing scientific methods for cyber security. *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results*. LASER `12.
- Colesky, M., & Ghanavati, S. (2016). *Privacy Shielding by Design - A Strategies Case for Near-Compliance*. 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), 271-275 Sep.
- Damore, K. (2017, Juni 21). How Physical Access Systems will be affected by GDPR. *IFSEC Global*. Hämtad 2018-04-23 från <https://www.ifsecglobal.com/physical-access-systems-will-affected-gdpr/>.
- Datainspektionen. (2018). *Dataskyddsreformen, allt om dataskyddsförordningen (GDPR)*. Hämtad 2018-02-06 från <https://www.datainspektionen.se/dataskyddsreformen/>.
- Denscombe, M. (2016). *Forskningshandboken. För småskaliga forskningsprojekt inom samhällsvetenskaperna*. Studentlitteratur AB, Lund.
- Denzin, N., & Lincoln, Y. (2005). *Introduction: The discipline and practice of qualitative research*. In N. Denzin & Y. Lincoln (Eds.), *The Sage handbook of qualitative research* (3rd ed.) (pp. 1-32). Thousand Oaks, Sage.
- Foster, R.D. (2010). Resistance, Justice and Commitment to Change. *Human Resource Development Quarterly*, vol. 21(1):3-39.
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (n.d). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, 16(1), 15-31.
- Hadziliadis, E. A., & NTUA, E. (2011). *Qualitative and Mixed Research Methods*.
- Herzberg, F. (1959). *The motivation to work*. New York: Wiley.

Internet of Things and People. (u.å.). *Research Area: Embedded Intelligence*. Hämtad 2018-02-08 från: <http://iotap.mah.se/embedded-intelligence/>.

IT Governance Privacy Team. (2016). *EU General Data Protection Regulation (GDPR) - An implementation and compliance guide*. IT governance publishing, Cambridgeshire.

Jacobsen, D. I., Thorsvik, J. (2008) *Hur moderna organisationer fungerar*. Studentlitteratur, Hungary.

Jacobsson, A., Boldt, M. och Carlsson, B. 2016. A risk analysis of a smart home automation system. *ScienceDirect. Future Generation Computer Systems* 56. 719-733. Doi:2015.09.003.

Long, K. (2017). GDPR threatens to catch third parties off guard. *Euromoney Institutional Investor PLC*. 48/584. 20-20.

Junwoo, S., Kyoungmin, K., Mookyu, P., Moosung, P. & Kyungho, L. (2017) *An Analysis of Economic Impact on IoT under GDPR*. 2017 International Conference on Information and Communication Technology Convergence (ICTC) Information and Communication Technology Convergence (ICTC), 2017 International Conference on. :879-881 Oct, 2017.

Kjellin, N. [softhouse tube]. (2018.02.02.). *Softhouse Education - Niclas Kjellin pratar GDPR (Ready, Steady, Code!)* [Videofil]. Hämtad 2018-04-15 från <https://www.youtube.com/watch?v=IQiEaYf72ls>.

Lindqvist, J. (2017). *New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?* International Journal of Law and Information Technology, Volume 26, Issue 1, Pages 45-63. Doi: 10.1093.

McCracken, G. (1988). *The long interview*. Sage Publishing, Canada.

Nieuwdorp, E. (2007). The Pervasive discourse: An analysis. *Computers In Entertainment*, 5(2), doi:10.1145/1279540.1279553.

O'Brien, R. (2016). Privacy and security: The new European data protection regulation and it's data breach notification requirements. *SAGE journals*, 33(2), 81-84. DOI: 10.1177/0266382116650297.

PCWorld from IDG. (2016). *Over SUS31bn invested in IoT startups in 2011-2015: Ovum*. Hämtad 2018-02-04 från <https://www.pcworld.idg.com.au/article/597988/over-us31bn-invested-iot-startups-2011-2015-ovum/>.

Robson, C. (2016) *Real World Research*. John Wiley & Sons Ltd, London.

Rouse, M. (2016, Juli). Internet of Things (IoT). *TechTarget*. Hämtad 2018-02-08 från <http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>.

Sandholm, L. (2012). *Kvalitetsstyrning med total kvalitet - Verksamhetsutveckling med fokus på total kvalitet*. Studentlitteratur AB, Lund.

Sentor. (2017) *Svenskarnas syn på IT-säkerhet*. Hämtad 2018-02-28 från https://www.sentor.se/wp-content/uploads/2017/08/Svenskarnas_syn_pa_it-sakerhet_2017.pdf.

Sentor. (2018) *6 av 10 upplever brister i svenska organisationers hantering av personuppgifter*. Hämtad 2018-02-28 från <http://news.cision.com/se/sentor-mss-ab/r/6-av-10-upplever-brister-i-svenska-organisationers-hantering-av-personuppgifter,c2333480>.

Sherwood, J., Clark, A. & Lynas, D. (2005). *Enterprise Security Architecture - A Business-Driven Approach*. Taylor & Francis Group, Boca Raton.

Sims, R. R. (2002). *Employee involvement is still the key to successfully managing change*. Westport: Quorum Books.

Sommerville, I. (2011). *Software Engineering*. Pearson Education, Addison-Wesley.

Sun, W. & Schmidt, C. (2018). Practitioners`Agile-Methodology Use and Job Perceptions. *IEEE Software*. 35(2):52-61 Apr, 2018. DOI: 10.1109/MS.2018.1661333.

Tankard, C. (2016) *What the GDPR means for businesses*. ScienceDirekt. Network Security. Doi: 10.1016/S1353-4858(16)30056-3.

Oliveira, L.B., Pereira, F.M.Q., Misoczki, R., Aranha, D. F. , Borges, F. & Liu J. The Computer for the 21st Century: Security & Privacy Challenges after 25 Years. (2017). *2017 26th International Conference on Computer Communication and Networks (ICCCN), Computer Communication and Networks (ICCCN), 2017 26th International Conference on*, 1. doi:10.1109/ICCCN.2017.8038394.

Cummings, R. The evolution of information assurance. (2002). *Computer*, (12), 65. doi:10.1109/MC.2002.1106181.

Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Nießner, M. (2016, June). Face2face: Real-time face capture and reenactment of rgb videos. In *Computer Vision and Pattern Recognition (CVPR), 2016 IEEE Conference on* (pp. 2387-2395). IEEE.

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

Yukl, G. (1999). An Evaluative Essay on Current Conceptions of Effective Leadership. *European Journal of Work and Organizational Psychology*. Doi: 10.1080/135943299398429.

Wästerfors, D. (2008). Analytiska knep. In K. Sjöberg & D. Wästerfors (Eds.), *Uppdrag forskning* (pp. 66 - 84). Liber, Stockholm.

Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *ScienceDirect*, 6, 1-20. DOI: 10.1016/S1353-4858(17)30060-0.

10. BILAGOR

Bilaga 1 - Information om studiens syfte skickat till respondenter

Hej XX,

Våra namn är Andrea Lukacs och Malgorzata Szczurek. Vi går IT och Ekonomi programmet på Malmö Universitet och ska nu skriva examensarbete inom Informatik. Vi skulle väldigt gärna vilja samla vår empirisk data hos XX! Jag bifogar våra CV till Dig, så ni får en bild av vilka vi är.

Jag var i kontakt med XX som tyckte att vårt examensarbete låter spännande, och föreslog att vi skulle ta kontakt med Dig. Vi tänkte därför fråga om du har möjlighet att ställa upp för en kort intervju?

Datainsamlingen kommer att ske i enlighet med Vetenskapsrådets (2017) etiska riktlinjer och därför kommer vi säkerställa ett informerat samtycke från respondenterna och alla respondenter och företaget kommer att anonymiseras.

Vårt ämne är följande:

Sammanfattningsvis vill vi skriva om etiska aspekter med IoT, med avgränsning till smarta larm. Vi vill undersöka hela processen, från tillverkning av kameror som ingår i systemet (empirin samlas in hos tillverkande företag), till deras försäljning, uppkoppling och drift (empirin samlas in hos larmföretag). Det vi hoppas ta reda på är vilka strategier ert företag använder i värdekedjan för att upprätthålla dataintegritet, samt hur strategierna förändras nu när GDPR ska träda i kraft. Vårt mål är att överlämna ett bidrag till Er när vi är färdiga i maj, vilket vi hoppas Ni kan få användning av!

Följande exempelfrågor har vi tänkt att ställa till Dig under intervjun:

- Hur arbetar ni för att förhindra att obehöriga kommer åt data?
- Görs det några kopior på databasen med användarnas uppgifter?
- Hur skyddar ni er mot dataläckor? Vad gör ni om en eventuell dataläcka inträffar?
- Vilka förändringar i kamerornas processer har ni infört för att uppfylla GDPR kraven?
- Finns det något som GDPR inte skyddar mot som kan vara en potentiell fara för integritet?

Vi är väldigt flexibla när det gäller tidpunkt för intervjuer, och uppskattar en längd på ca 1 timme. Vi skulle uppskatta ert samarbete väldigt mycket, och vill gärna lämna över en kopia på vårt examensarbete i maj till Er, vilket vi önskar ni får användning av inom er verksamhet.

Med vänliga hälsningar,
Andrea och Malgorzata

Bilaga 2 - Samtyckesblankett för intervjuer

Samtyckesblankett för intervju

Denna samtyckesblankett är för personer involverade i utvecklingsprocessen av smarta larm som vi bjuder in till att medverka i studien av dataintegriteten hos smarta kameror.

Andrea Lukacs och Malgorzata Szczurek
Malmö Universitet
Examensarbete

Denna samtyckesblankett har två delar:

- **Informationsblad (för att dela information om studien med dig)**
- **Godkännandeintyg (för signaturer om du väljer att delta)**

Del I: Informationsblad

Introduktion

Vi heter Andrea Lukacs och Malgorzata Szczurek och studerar till kandidatexamen i Informatik. Vi forskar kring dataintegriteten av smarta kameror för att kunna komma fram till ett ramverk för utvecklingsprocesser av liknande produkter. Vi vill informera dig om och bjuda in dig till att medverka i forskningen. Denna samtyckesblankett kan innehålla ord som du inte förstår. Be oss att stanna när vi går genom informationen så kan vi förklara. Om du har frågor senare kan du ställa dem till oss eller en annan forskare.

Målet med forskningen

Vi vill undersöka hur dataintegritet säkerställs genom hela kedjan från utvecklingen av mjukvaran i kameror till uppkopplingen till resten av larmsystemet. Vi tror att du kan hjälpa oss genom att berätta om på vilket sätt du och dina arbetskamrater arbetar med detta och hur processen för detta ser ut. Vi vill även lära känna strategier som används för att säkerställa att produkterna följer GDPR lagen.

Typ av deltagande

Denna forskning innebär att du deltar i en intervju som tar ungefär en timme.

Deltagarval

Du har bjudits in att delta i denna forskning eftersom vi anser att din arbetserfarenhet kan bidra mycket till vår förståelse.

Frivilligt deltagande

Ditt deltagande i denna forskning är helt frivilligt. Det är ditt val om du vill delta eller inte. Valet du gör kommer inte ha någon betydelse för dig eller ditt jobb. Du kan ändra dig senare och sluta delta även om du kom överens om det tidigare.

Varaktighet

Forskningen pågår under 10 veckor. Under denna tid kommer vi genomföra en intervju med dig som tar ca en timme.

Risker

Det finns en risk att du delar med dig av personlig eller konfidentiell information av en slump, eller att du kanske känner dig obekvämd med att prata om några av ämnena. Vi vill dock inte att detta ska ske. Du behöver inte svara på någon fråga eller delta i intervjun om du

känner att frågan eller frågorna är för personliga eller om du blir obekvämd av att svara på dem.

Förmåner

Det kommer inte finnas några förmåner för dig men ditt deltagande kommer sannolikt att hjälpa oss att ta reda på mer om arbetet med dataintegriteten.

Ersättning

Du kommer inte få någon ersättning för att delta i forskningen.

Sekretess

Forskningen som genomförs kan dra till sig uppmärksamhet och om du deltar kan du få frågor från andra människor. Vi kommer inte dela någon information om dig till någon utanför forskargruppen. Den information vi samlar in från detta forskningsprojekt kommer att hållas privat. Ditt namn kommer inte komma upp i rapporten och endast forskarna kommer veta att information handlar om just dig. Denna kunskap kommer inte att delas med någon.

Rapportering av resultatet

Inget som du berättar för oss idag kommer att delas med någon utanför forskargruppen, och inget kommer att tillskrivas ditt namn. Kunskapen som vi får från denna forskning kommer att delas med dig innan den görs tillgänglig för allmänheten. Varje deltagare kommer få en sammanfattning av resultaten. Slutligen publicerar vi resultaten så att andra intresserade människor kan lära av forskningen.

Rätt att vägra eller dra sig ur

Du behöver inte delta i denna forskning om du inte vill göra det. Du kan avbryta deltagandet i intervjun när som helst om du önskar. Vi kommer att ge dig möjlighet att i slutet av intervjun se över dina kommentarer och du kan be om att ändra eller ta bort delar av dem om du inte håller med våra anteckningar eller om vi inte förstod dig korrekt.

Vem ska du kontakta

Om du har några frågor kan du ställa dem nu eller senare. Om du vill ställa frågor senare kan du kontakta någon av följande: Malgorzata Szczurek, malgorzataszczurek@hotmail.com eller Andrea Lukacs, andrea.lukacs@hotmail.se

Du kan fråga oss om någon del av forskningsstudien, om du vill.

Har du några frågor?

Del II: Godkännandeintyg

Jag har blivit inbjuden att delta i forskning om dataintegritet hos smarta kameror.

Jag har läst ovanstående information, eller så har den lästs för mig. Jag har haft möjlighet att ställa frågor om den och alla frågor jag har ställt har besvarats till min tillfredsställelse. Jag samtycker frivilligt till att vara deltagare i denna studie.

Namn på deltagare _____

Deltagarens signatur _____

Datum _____

Dag/månad/år

Forskarens uttalande

Jag har noggrant sett till att den potentiella deltagaren har läst eller har läst ut informationsbladet till den potentiella deltagaren och till mina bästa möjliga förutsättningar sett till att deltagaren förstår att följande kommer ske:

- 1. Intervjun kommer genomföras.**
- 2. Resultatet kommer delas med deltagaren innan den publiceras.**
- 3. Resultatet kommer inte kopplas till deltagarens namn på något sätt.**

Jag bekräftar att deltagaren fick möjlighet att ställa frågor om studien, och alla frågor som ställts av deltagaren har besvarats korrekt och till vår bästa förmåga. Jag bekräftar att individen inte har tvingats att ge sitt samtycke, och samtycket har givits fritt och frivilligt.

Underskrift av forskare _____

Datum _____

Dag/månad/år

Bilaga 3 - Frågor till intervjuer

Respondent 1:

- Hur ser utvecklingsprocessen för en kamera (till smarta larm) ut? Skiljer det sig mellan länderna?
- Vill du ge exempel på kraven som ni ställer på era produkter?
- Hur säkerställer ni dataintegriteten vid utvecklingen av en smart larm?
- Hur går det till om det upptäcks fel som behöver rättas till i era produkter?
- *Hur ofta ger ni ut uppdateringar av mjukvaran i kamerorna? Uppdateras kameror automatiskt? Behöver man skriva in någon kod eller finns det någon annan form av autentisering för att mjukvaran ska kunna uppdateras?*
- *Arbetar testare på databasen där användarnas riktiga uppgifter finns?*
- *Använder ni er av kryptering av datan?*
- Vilka förändringar har ni infört i utvecklingsprocessen för att uppnå GDPR kraven? Planerade förändringar?
- Vilken är den största utmaningen med GDPR enligt Dig? Hur kommer ni att hantera det?
- *Vilka utmaningar eller svårigheter tror du kan finnas efter GDPR strategin är implementerad?*
- Hur kommer ni att följa upp att GDPR kraven efterlevs på företaget?
- Finns det något som GDPR inte skyddar mot som kan vara en potentiell fara för integritet? (GDPRs brister)
- Ser du GDPR som en begränsning eller en möjlighet? Varför?
- Finns det något mer du vill tillägga?

Respondent 2:

- Vill du beskriva utvecklingsprocessen av kameror som installeras i smarta larm?
- Vilka avdelningar och roller som är involverade i processen?
- Hur jobbar ni med dataintegritet vid utvecklingen? Vill du ge exempel på utmaningar med dataintegritet av smarta kameror?
- Hur arbetar ni för att förhindra att obehöriga kommer åt data?
- Hur går det till om det upptäcks fel som behöver rättas till i era produkter?
- Hur ofta ger ni ut uppdateringar av mjukvaran i kamerorna?
- Arbetar testare på databasen där användarnas riktiga uppgifter finns?
- Hur skyddar ni er mot dataläckor? Vad gör ni om en eventuell dataläcka inträffar?
- Vilka förändringar kommer ni att införa i utvecklingsprocessen för att uppnå GDPR kraven?
- Vilka förändringar har ni redan infört i utvecklingsprocessen på grund av GDPR?
- Vilka utmaningar eller svårigheter tror du kan finnas efter GDPR strategin är implementerad?
- Finns det något mer du vill tillägga?

Respondent 3:

- Hur säkerställer ni dataintegriteten vid utvecklingen av smarta kameror (som ingår i smarta larm systemet)?
- Hur skyddar ni er mot dataläckor? Vad gör ni om en eventuell dataläcka inträffar?
- Hur går det till om det upptäcks fel som behöver rättas till i era produkter?
- Vad har ni för strategi för att uppfylla GDPR kraven?
- Vilka förändringar har ni infört i utvecklingsprocessen för att uppnå GDPR kraven?
- Vad finns det för utmaningar med att implementera GDPR kraven?

- Svåraste GDPR kraven? Berätta! Hur löser ni det?
- Hur kommer ni att följa upp att kraven efterlevs i företaget? (efter att GDPR träder i kraft)
- Finns det något som GDPR inte skyddar mot som kan vara en potentiell fara för integritet?

Respondent 4:

- Kan ni beskriva hur systemet fungerar (smarta larm)?
- Hur hanteras bilder som kameran tar? *Vilka har tillgång till bilderna? Hur länge förvarar ni dem?*
- Hur ser datans livscykel ut som kamerorna bearbetar? *Hur förvaras data? Är användarnas uppgifter anonymiserade?*
- Görs det några kopior på databasen med användarnas uppgifter?
- Hur går uppdateringar till?
- Hur arbetar ni för att förhindra att obehöriga kommer åt data?
- Hur skyddar ni er mot dataläckor? *Vad gör ni om en eventuell dataläcka inträffar?*
- Vilka personer tittar på bilder från kameran? Kan personer som tittar på bilder för att avgöra om inbrott har skett spara bilderna de tittar på? *Vet de vad husets ägare heter eller vilken adress den befinner sig på?*
- Hur är gruppen som jobbar med gdpr frågorna och förberedelserna är sammanställd?
- Vilka förändringar har ni infört för att uppfylla GDPR kraven?
- Hur ska ni följa upp att gdpr kraven efterlevs då på företaget?
- Vad tycker du är den största utmaningen med gdpr enligt dig?
- Hur ser du på gdpr, som en begränsning eller en möjlighet för företaget och varför?
- Finns det något som GDPR inte skyddar mot som kan vara en potentiell fara för integritet?
- Vi vill gärna fråga om det finns något du vill tillägga någonstans?
- Finns det någon dokumentation som vi skulle kunna titta på som behandlar integritet och datasäkerhet?

Respondent 5:

- How do you think that GDPR will affect companies developing IoT products?
- To what degree do you think the companies meet the requirements already?
- What will they have to change in the processes for developing products to meet all the requirements?
- What challenges or difficulties will there be in the processes for developing products when it comes to data integrity?
- Is there something that GDPR does not protect against that could be a potential danger for integrity?

Respondent 6:

- Till vilken grad tror du att företag redan uppnådde GDPR krav innan det föreslogs?
- Hur påverkar GDPR livscykeln av data som smarta kameror genererar?
- Vad tror du företag behöver förändra i sina utvecklingsprocesser av smarta kameror för att uppfylla GDPR kraven?
- Vilka utmaningar/svårigheter kan finnas i utvecklingsprocesser när det gäller dataintegritet?
- Hur ser det ut att implementera GDPR kraven i en IoT kontext? *Hur skiljer det sig från andra områden?*
- Vilka roller som är involverade i en IoT kontext (datakontrollant, dataproducent,..) och vilket ansvar har dessa?

- Hur hanterar företag till exempel notifikationer om dataintegritet (när användare ska ge tillåtelse att använda data) i en IoT kontext?
- Hur hanteras sekundär användning av data? (användning i syften andra än de som kunder har gett samtycke till)
- Vad händer om företaget finns i Sverige men hanterar data i Kina t.ex.? *Finns det andra sätt att komma runt GDPR på?*
- Tycker du att GDPR ger tillräckligt tydliga instruktioner?
- Hur ser du på GDPR: som en möjlighet eller en begränsning för företag som jobbar med smarta kameror? *Varför?*
- Finns det något som GDPR inte skyddar mot som kan vara en potentiell fara för integritet eller säkerhet? (GDPRs brister)
- Har du tips på mer konkreta riktlinjer som företag hade kunnat använda sig av?