LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Attityder till integritet från ett utvecklarperspektiv

En studie om hur systemutvecklare i den offentliga sektorn behandlar integritet

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Agnes Larsson
Mana Vakil

Handledare: Markus Lahtinen

Rättande lärare: Björn Svensson
Odd Steen

Attityder till integritet från ett utvecklarperspektiv: En studie om hur systemutvecklare i den offentliga sektorn behandlar integritet

ENGELSK TITEL: Attitudes towards integrity from a developer perspective: A thesis on how developers in the public sector conceptualize privacy

FÖRFATTARE: Agnes Larsson och Mana Vakil

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Christina Keller, Professor

FRAMLAGD: maj, 2021

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 74

NYCKELORD: Privacy by Design, Digital integritet, Systemutvecklare, Systemutvecklingsprocessen, Integritetshantering, Offentlig sektor

SAMMANFATTNING (MAX. 200 ORD):
Personlig integritet på nätet har på den senaste tiden blivit ett allt mer omtalat ämne vilket skapat engagemang men också oro hos många internetanvändare. Eftersom systemutvecklarna är de som designar och därmed har viss makt över dessa produkter har vi valt att fokusera denna studie på just systemutvecklare. Syftet med studien är att få en bättre insyn i systemutvecklares attityd gentemot integritet för att därigenom kunna se om, och i så fall hur, de arbetar med detta i systemutvecklingsprocessen. Studiens metod består av intervjuer av fem systemutvecklare på en verksamhet inom den offentliga sektorn. Resultatet visade att det inte finns något vidare intresse för integritetshantering längre än vad som krävs av gällande lagstiftning. Studien visade även att systemutvecklare tenderar att se på integritet som ekvivalent med GDPR. De systemutvecklare som uttryckte en större oro över bristen på integritet på nätet var även de som reflekterade mer över detta inom sin yrkesroll.

Innehåll

Tabeller

1 Introduktion

1.1 Bakgrund

Personlig integritet på nätet har på den senaste tiden blivit ett allt mer omtalat ämne. Det produceras allt fler artiklar inom området vilket ökat allmänhetens medvetenhet om hur deras personliga data egentligen samlas in och används. Det blir även allt vanligare att i dessa artiklar instruera användaren hur denne kan begränsa tjänstens dataåtkomst eller till och med uppmana användaren att radera tjänsten. I tidningsartikeln *Do You Suddenly Need To Stop Using Facebook?* diskuterar Doffman (2021) om hur Facebook har en policy som hindrar annonsörer från att göra vissa antaganden om bland annat användarens etnicitet, religion och sexuella läggning i annonsen. Att man inte får rikta annonser på det här sättet betyder dock inte att Facebook inte har den här informationen om dig. Facebook använder fortfarande datan och riktar sig mot människor baserat på den, de ser bara till att dölja detta från användarna genom att inte nämna det i annonsen (Doffman, 2021). Artiklar som dessa har således också ökat både intresset och oron för vilken data som samlas in. Det ökade intresset och ifrågasättandet har resulterat i att det instiftats olika lagar i ett försök att tvinga företag till bättre, mer etisk databehandling som i sin tur ska skydda individers integritet.

Med målet att bättre kunna kontrollera och reglera databehandling och därmed skydda personers integritet på nätet har flertalet lagar och regelverk skapats. I maj 2018 trädde EU General Data Protection Regulation (GDPR) i kraft. Det är en lagstiftning som reglerar hur personuppgifter ska samlas in och användas (Nationalencyklopedin, n.d. a). Förordningen ersatte de tidigare dataskyddsdirektiv som fastslogs 1995. Ändringarna var omfattande och gäller hela EU samt de företag och verksamheter som har EU-medborgare som kunder eller medlemmar. GDPR:s huvudsyfte är att ge individer ökad kontroll kring sina personuppgifter. Förordningen hindrar hantering av personuppgifter om laglig grund saknas. Sverige valde att införa en ny dataskyddslag i samband med GDPR. Detta för att ytterligare komplettera GDPR.

Det är speciellt viktigt för verksamheter inom den offentliga sektorn att efterleva GDPR eftersom de i stor utsträckning hanterar känsliga personuppgifter. När en verksamhet inom den offentliga sektorn behandlar personuppgifter måste den iaktta tre huvudprinciper: rättvis och lagenlig behandling, ändamålsbegränsning och uppgiftsminimering och uppgiftslagring (Europeiska kommissionen, n.d. a). Innan dessa uppgifter behandlas måste även de enskilda personerna bli informerade om detta. En skillnad mellan verksamheter inom den privata och offentliga sektorn är att verksamheter inom den offentliga sektorn alltid är skyldiga att utse ett dataskyddsombud som ser till att lämpliga åtgärder har genomförts för att säkra personuppgifter (Europeiska kommissionen, n.d. b).

Inte minst direktiv som GDPR påvisar tydligt att frågan om integritet har blivit en nyckelfråga inom den allt mer digitaliserade världen. Som enskild individ är det svårt att påverka detta och det krävs ofta regelverk och riktlinjer på nationella nivåer. Problemet är att det ofta tar lång tid

att få igenom lagar och ändringar. De som har störst inflytande blir därför företagen som erbjuder de digitala tjänsterna samt de enskilda systemutvecklarna som tar fram produkterna. Även om det inte alltid är systemutvecklarna själva som tar designbesluten är det deras ansvar att se till att dessa efterlevs. Ett sätt att reducera riskerna kring digital integritet kan således vara genom att få systemutvecklare att prioritera integritet och säkerhet. Lawrence Lessig skriver i sin bok Code 2.0 följande om att reglera kod:

> As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature (Lessig, 2009, s. 155).

Dålig integritetshantering behöver dock inte bero på att systemutvecklarna inte vill ta ansvar eller inte bryr sig. Det kan likväl bero på att det ibland är svårt för systemutvecklare att följa designbeslut. Designbesluten tenderar att inte vara direkt kopplade till just koden, vilket gör att de blir svåra för systemutvecklarna att förhålla sig till. Den utvecklade produkten eller tjänsten är ju förkroppsligandet av besluten som tagits av systemutvecklarna, och dessa tillsammans avgör i hur stor grad mjukvaran uppfyller sina krav (Mehrpour, LaToza & Kindi, 2019). Om systemutvecklarna inte kunnat följa designbesluten helt och hållet får vi därmed en mjukvara som inte uppfyller de uppsatta kraven. Det finns således flertalet anledningar till att system ibland tenderar att ha bristfällig integritetshantering och inte lever upp till de designbeslut som finns.

1.2 Problemområde

Den problematiska aspekten med integritet och systemutveckling är att det finns många riktlinjer som alla är svåra att efterleva. Riktlinjerna är ofta väldigt teoretiska och saknar en konkret förklaring för hur man uppnår ett optimalt integritetsskydd. Därmed saknas det en generell praxis för hur systemutvecklare ska hantera och inkorporera integritet vilket leder till att det blir en tolkningsfråga. I denna tolkningsfråga verkar det inte råda konsensus bland olika verksamheter, eller ens enskilda systemutvecklare, gällande vad som är den rätta nivån på integritetsskydd. Hanteringen av integritet i systemutvecklingsprocessen kan därför skilja sig åt väldigt mycket från en verksamhet till en annan. Dessutom har det visat sig att systemutvecklare är mer villiga än användare att acceptera ett sämre integritetsskydd för att få en bättre funktionalitet (Hadar et al., 2018), vilket också är problematiskt. Även om specifika designbeslut har fattats för att uppnå en bra integritetshantering riskerar dessa alltså att åsidosättas när integriteten kompromissas till fördel för funktionaliteten.

Även om man som systemutvecklare vill ta ansvar för en säker datahantering är det alltså inte alltid helt lätt. Bristen på systematiska tillvägagångssätt för att samla in användarnas integritetskrav gör att systemutvecklare ofta behöver designa applikationer antingen baserat på sina egna antaganden om användarnas förväntningar på integritet eller baserat på deras egna förväntningar på integritet ur ett användarperspektiv (Senarath & Asanka, 2018). Det är dock lätt hänt att dessa två smälter ihop. Systemutvecklare gör alltså antaganden om användarens förväntningar men färgas i dessa antaganden av sina egna erfarenheter och förväntningar. Oftast stämmer en systemutvecklares förväntningar inte överens med en faktisk användares förväntningar även om systemutvecklaren har ett användarperspektiv. Detta gör att systemen sällan reflekterar användarnas krav och förväntningar.

Problemet märks tydligt i litteraturen inom ämnet, eller rättare sagt avsaknaden av litteratur inom ämnet. Det har gjorts många olika studier om slutanvändare och deras integritetsuppfattning. Däremot har det riktats betydligt mindre uppmärksamhet på själva processen där integritet faktiskt blir en del av olika informationssystem samt systemutvecklarnas roll i integritetshanteringen (Hadar et al., 2018). Att forskning rörande digital integritet i systemutvecklingsprocessen saknas blir problematiskt då det är i systemutvecklingsprocessen som man har en chans att göra skillnad. Antón, Earp & Young skrev 2010 en artikel där de skulle utreda hur internetanvändares oro över integritet hade utvecklats sedan 2002. Intressant nog kom de fram till att individers primära oro fortfarande var densamma som 2002, men att själva orosnivån nu var högre. Man kan därmed dra slutsatsen att i takt med att vi blir mer medvetna blir vi också mer oroliga. Detta talar för att det borde läggas mer fokus på integritet i systemutvecklingsprocessen. Vi kan dock inte förändra en process som vi inte har en aning om hur den fungerar. Utan att veta hur systemutvecklare arbetar med och ser på integritet i dagsläget är det ytterst svårt att göra förändringar.

Målet med den här studien är att studera den litteratur som finns om hur man som systemutvecklare kan arbeta med integritet och jämföra detta med hur systemutvecklare faktiskt arbetar med integritet som en del av systemutvecklingsprocessen.

1.3 Forskningsfrågor

Baserat på den litteratur som finns inom området och det identifierade problemområdet ämnar vi besvara följande forskningsfrågor:

Hur aktivt är integritetstänket bland enskilda systemutvecklare i systemutvecklingsprocessen?

På vilket sätt genomsyrar de enskilda systemutvecklarnas egna erfarenheter och preferenser integritetstänket?

1.4 Syfte

Syftet med uppsatsen är att med hjälp av semistrukturerade intervjuer av systemutvecklare från en verksamhet inom den offentliga sektorn undersöka hur integritet behandlas i systemutvecklingsprocessen. Det vi främst är intresserade av är hur systemutvecklarna arbetar med integritet i systemutvecklingsprocessen idag; var i processen detta kommer in, vilka specifika aktiviteter som är en del av integritetshanteringen samt hur de prioriterar integritet i förhållande till annan funktionalitet. Genom att ta reda på detta ämnar vi bidra till den i nuläget ringa forskningen som finns inom området. Förutom detta hoppas vi att uppsatsen bidrar till att ge en ökad förståelse för hur systemutvecklare arbetar med integritet i sitt dagliga arbete, och varför de arbetar som de gör.

1.5 Avgränsningar

Vi avgränsar oss till att endast undersöka en verksamhet inom den offentliga sektorn. Vi avgränsar oss även från att presentera lösningar på eventuella utmaningar som identifieras.

2 Litteraturgenomgång

Litteraturgenomgången är uppdelad i sju olika delar. Kapitlet inleds med hur systemutvecklare ser på integritet som en del av systemutvecklingsprocessen idag. Sedan följer en genomgång av Privacy by Design som är ett omtalat ramverk för integritetshantering. Efteråt görs en kritisk granskning av ramverket där olika utmaningar med att applicera principerna i praktiken presenteras. Därefter återges hur integritet vanligen inkorporeras i systemutvecklingsprocessen för att sedan presentera de brister som finns gällande systemutvecklares integritetshantering. Litteraturgenomgången avslutas med en genomgång av Privacy Impact Assessment, ett verktyg för att skydda integritet, för att sedan sammanfatta genomgången i tabellformat (se Tabell 1).

2.1 Systemutvecklares syn på integritet

Hur systemutvecklare ser på integritet har en betydelsefull roll för systemutvecklingen. Om det är något som inte prioriteras eller helt enkelt inte ses som viktigt av systemutvecklaren kommer detta speglas i systemet. Studier har visat att det finns ett stort gap mellan integritet sett från de juridiska normerna och hur det upplevs av systemutvecklare (Hadar et al., 2018). Systemutvecklare ser på integritet som ett teoretiskt, abstrakt och opraktiskt koncept (Hadar et al., 2018). Vissa beskriver det till och med nästan som ett naivt koncept, och den generella skepticismen bland systemutvecklare till begreppet integritet blir då väldigt tydlig.

Många blir även obekväma av att diskutera integritet då de är något osäkra på vad som egentligen menas med begreppet och samtidigt väldigt ifrågasättande till genomförbarheten av inbäddad integritet (Hadar et al., 2018). Huruvida denna osäkerhet kommer från bristfällig kommunikation och utbildning kring integritet från ledningens sida eller om det beror på något annat är oklart. Något som annars kan bidra till osäkerheten är att systemutvecklare ser på integritet ur fel synvinkel. Trots sitt i övriga tekniska synsätt tenderar nämligen systemutvecklare att diskutera integritet som ett socialt problem snarare än ett tekniskt problem, vilket antyder att integritetsbeslut beror mer på sociala normer än lagar eller tekniska riktlinjer (Hadar et al., 2018).

Trots den skeptiska inställningen till integritet visade det sig i en studie gjord av Senarath & Asanka (2018) att systemutvecklare anser att fler dataelement är känsliga än vad användarna gör. Till exempel såg inte användarna sin kreditkortsdata som känslig medan systemutvecklarna gjorde det. Bland de dataelement som identifierats som känsliga av dataskyddsföreskrifter ansåg inte heller användarna att vare sig nationalitet eller ras var känslig data medan systemutvecklarna identifierade alla dataobjekt som fanns i föreskrifterna som känsliga. Senarath & Asanka (2018) tror att detta kan bero på att systemutvecklare är mer medvetna om de integritetsrisker som finns och därav har en bättre förståelse för effekterna av dataförlust.

2.2 Privacy by Design

Personen som myntade uttrycket Privacy by Design är Ann Cavoukian. Cavoukian har bland annat skrivit ett dokument (2009) om sju grundläggande principer för implementering av Privacy by Design. Privacy by Design bygger på Fair Information Practices men innefattar en betydande höjning av gränsen för integritetsskydd. Artikeln är menad att fungera som ett universellt ramverk för hur man bäst skyddar integritet (Cavoukian, 2009).

1. **Proactive not Reactive; Preventative not Remedial**
   Den första principen utgår från att man måste lösa så många problem som möjligt innan de hinner uppstå. För att uppnå detta krävs ett stort engagemang och olika etablerade metoder för att kunna känna igen dålig integritetsdesign.

2. **Privacy as the Default Setting**
   Den andra principen bygger på att användaren inte ska behöva vidta några åtgärder för att skydda sin integritet. Integritetsskyddet ska vara inbyggt i systemet och finnas där utan att användaren behöver göra något.

3. **Privacy Embedded into Design**
   Den tredje principen menar att Privacy by Design ska vara inbäddat i systemet och något man har i åtanke under hela processen. Det ska inte vara något man bara lägger till när systemet är färdigt.

4. **Full Functionality – Positive-Sum, not Zero-Sum**
   Den fjärde principen handlar om att Privacy by Design inte ska hindra annan funktionalitet. Integritet tvingas ofta tävla mot andra krav, intressen och mål. Man måste alltså även försöka tillgodose andra legitima mål för att uppnå hög funktionalitet.

5. **End-to-End Security – Full Lifecycle Protection**
   Den femte principen gäller säkerhet. Utan säkerhet finns det ingen integritet och för att kunna säkerställa ett visst integritetsskydd krävs därmed också hög säkerhet från början till slut. Det kan exempelvis gälla saker som att data hämtas på ett säkert sätt.

6. **Visibility and Transparency – Keep it Open**
   Den sjätte principen menar att det är viktigt med synlighet och transparens för att skapa ansvar och inge förtroende hos intressenterna. Det är också ett bra sätt att försäkra intressenter om att produkten fungerar enligt de mål man satt upp.

7. **Respect for User Privacy – Keep it User-Centric**
   Den sjunde och sista principen är att hålla systemet användarvänligt och individanpassad. Enligt Cavoukian själv är de bästa resultaten vanligtvis de som medvetet har designats utefter individuella användare.

2.3 Utmaningar med Privacy by Design

Även om Privacy by Design erbjuder principer för att underlätta implementeringen av inbäddad integritet vid systemutvecklingen så beskrivs principerna som vaga. De har därav

blivit kritiserade för att inte vara framtagna med ett tekniktänk i åtanke. Integritet har blivit ett av de viktigaste icke-funktionella kraven som finns för system idag. Martin, del Alamo & Yelmo (2014) menar på att även om det finns ramverk att följa saknar systemutvecklare många gånger detaljerade riktlinjer innehållandes tydliga instruktioner för implementering av de tekniska bitarna som krävs för att kunna få med inbäddad integritet i slutprodukten. Det är alltså inte ovanligt att systemutvecklare kritiserar Cavoukian för att ha utformat principer som är mer teoretiska än tekniska, som också lämnar utrymme för många frågor och oklarheter hos systemutvecklare. Hon anses inte göra tillräckligt arbete för att systematisera principerna.

Sarah Spiekermann (2012) skriver också om diverse utmaningar med fenomenet. Det krävs stöd och engagemang från både ledningen och systemutvecklarna. Hon menar att det kan bli svårt att få med sig ledningen då personlig data ofta är en stor tillgång i många organisationers affärsmodell. Utan tillgången till data är det också många tjänster som går förlorade. Som exempel ger hon reklamintäkter som ofta baseras på personlig data, såsom att spåra användares beteendemönster och liknande. Dessutom poängterar Spiekermann (2012) att datainsamling ofta används för att spåra kriminella personer och nätverk, vilket också kommer gå förlorat om vi minimerar våra digitala fotspår. Till slut ställer hon sig också frågan om det för en organisation egentligen finns några påtagliga fördelar med att investera i Privacy by Design.

Att ensamt applicera Privacy by Design är oftast inte tillräckligt heller. För att lyckas med implementering av principerna är det viktigt att organisationer känner ansvar kring människans integritet och sitt sätt att hantera personlig data. Professor Paul A. Schwartz (2009) poängterar att organisationer numera lägger mer resurser på att utbilda sina anställda och implementera en framtagen praxis för integritetshantering på företaget. Detta är essentiellt för att kunna uppnå öppenhet och ansvarstagande inom organisationen, som i sin tur ska leda till det högre säkerhetstänk man vill se inom organisationer. Ett ansvarstagande tänk inom organisationer definieras enligt Schwartz (2009) som ett tänk där man tar hänsyn till hur man behandlar personlig information och strävar efter att skydda individer från den skada som kan ske om data inte hanteras på ett säkert sätt.

Cavoukian, Taylor & Abrams (2010) ger företaget HP som exempel där man arbetade med att ta fram ett verktyg för ansvarstagande i organisationer. Tanken var att verktyget skulle kombinera de viktigaste principerna från tänket kring ansvarstagande och Privacy by Design vilket bekräftar Schwartz påstående kring ökade satsningar på organisationers ansvarstagande. Grundvärderingarna för ett fungerande ansvarstagande bygger på fem principer (Cavoukian, Taylor & Abrams, 2010):

1. Företags engagemang gällande ansvar och införandet av interna policies som överensstämmer med externa kriterier.
2. Förse organisationen med nödvändiga hjälpmedel såsom utbildning och andra verktyg för att kunna verkställa den bestämda säkerhetspolicyn.
3. System för att kunna göra uppföljningar och utvärderingar av arbetet.
4. Transparens och olika mekanismer för individuellt deltagande.
5. Medel för gottgörelse och extern förstärkning.

Företag bör ta hjälp av externa mätbara lagar och regelverk. Det är viktigt att implementera regelverken högt upp i organisationen. Författarna menar att man bör arbeta sig ner i organisationen och säkerställa att säkerhetspolicyn förstås och implementeras av alla anställda samt att interna uppföljningar görs kontinuerligt.

2.4 Integritet i systemutvecklingsprocessen

Till att börja med finns det olika sätt att hantera och inkorporera integritet i system. Främst pratar man om två olika sätt; *privacy-by-architecture* och *privacy-by-policy*. I *privacy-by-architecture* är systemets arkitektur designad för att bevara integritet, till exempel genom kryptering, anonymisering och decentralisering av data (Hadar et al., 2018). I *privacy-by-policy* är systemet konfigurerat, snarare än designat, för att stödja integritet. Några exempel på detta är användarkontroll, styra vem som har åtkomst och begränsa datainsamling (Hadar et al., 2018). Den främsta skillnaden mellan de två tillvägagångssätten är den olika säkerhetsgraden.

Hadar et al. (2018) förklarar att i *privacy-by-architecture* kan användarnas integritet inte kränkas ens om man skulle vilja det eftersom själva arkitekturen förhindrar sådana risker. *Privacy-by-policy* är däremot inte lika säkert då integritetsskyddet beror på hur systemet hanteras och vilka policies som systemoperatörerna har. Det finns dock ingen anledning att välja mellan de båda, utan det optimala är att först designa systemets arkitektur för att bevara integritet och sedan förbättra integriteten genom att konfigurera systemet för att stödja ytterligare integritetshantering. Man kan alltså se dem båda som ett komplement till varandra snarare än separata tillvägagångssätt.

Det har även gjorts en annan studie (Ayalon, Toch, Hadar & Birnhack, 2017) om hur systemutvecklare tar designbeslut gällande användarnas integritet. Med studien ville man få svar på hur stort inflytande systemutvecklare har när det kommer till att forma organisatorisk sekretesspraxis och hur de påverkar integritetsdynamiken. Studien visade att det organisatoriska klimatet gällande integritet påverkade besluten mer än den rättsliga bakgrunden. Ayalon et al. (2017) tror att detta kan bero på att klimatet förmedlar den rättsliga och affärsmässiga miljön som organisationen verkar i. Studien visade även att systemutvecklares egna erfarenheter som slutanvändare, och därmed deras personliga upplevelse av integritet, också påverkar designbesluten.

Man har tidigare påvisat att implementeringen av Privacy by Design ger en ökad säkerhet genom hela livscykeln för de utvecklade produkterna och är numera ett av de mest dominerande säkerhetsåtgärder som används. Bu, Jiang, Liang & Wang (2020) hävdar att det finns en tydlig koppling mellan incitament, hur systemutvecklare ser på Privacy by Design och användningen av principerna. Eftersom systemutvecklarna är de som ansvarar för det mesta av slutprodukten ser man ofta en reflektion av deras beteende och tankesätt i produkten. Om säkerhet är något de själva prioriterar högt är chansen större att produkterna de jobbar med också har hög säkerhet (Bu et al., 2020). Således påverkar systemutvecklarens preferenser produktens kvalitet till viss del.

Som tidigare nämnt har man upplevt att forskningsmaterial relaterat till systemutvecklares synsätt på implementering av Privacy by Design har varit begränsat. För att komplettera det existerande materialet frågade Bu et al. (2020) i sin studie 253 IT-anställda i Kina om de ansåg att Privacy by Design skulle öka deras arbetsbelastning. De frågade även om de trodde att individuella faktorer kunde influera hur de implementerade Privacy by Design. Insamlad data visade på att implementering av Privacy by Design ansågs bidra till ökad arbetsbelastning bland de anställda och var därför något många undvek. Då synsättet blev negativt försvårade detta implementeringen av principerna för Privacy by Design.

Studien från Bu et al. (2020) visade också att IT-anställdas intentioner gällande implementering av Privacy by Design är direkt kopplad till deras inställning gällande

implementationen av principerna. Om systemutvecklare känner att principerna kommer öka kvaliteten, prestandan och underlätta deras arbete är det större chans att de väljer att jobba på ett sätt som uppfyller kraven för Privacy by Design. De kan också enklare bemöta förändringarna som krävs vid genomförandet. Trots att många systemutvecklare var eniga om att detta ökade säkerheten för produkter så var de kritiska till den ökade arbetsbelastningen det kunde medföra. De associerade många gånger Privacy by Design med något negativt som skulle försämra deras möjligheter till bättre presterande på arbetsplatsen.

Bu et al. (2020) nämner även i sin studie att de i tidigare intervjuer sett att alla som jobbar inom området inte känner till och besitter tillräckligt med kunskaper kring Privacy by Design. Paralleller som dragits mellan principerna och ökad arbetsbelastning såg man inte bland individerna med bristfällig kunskap inom principerna. Man kunde däremot dra slutsatsen att mängden kunskap inom ämnet är avgörande för hur man ser på implementeringen av principerna, samt hur mottagliga de är för förändringarna. En ökad förståelse för Privacy by Design resulterade i en mer mottaglig syn på implementeringen. Även kollegors syn på Privacy by Design påverkar hur enskilda individer tänker kring användandet av principerna. Större acceptans på arbetsplatsen och bland kollegorna leder till ökat intresse för den enskilda systemutvecklaren. Bland systemutvecklarna såg Bu et al. (2020) också att uppmuntran till belöningar, hot eller andra påföljder påverkade och ibland kontrollerade hur de tänkte kring implementeringen av Privacy by Design. Man kunde se att om någon annan blev belönad kunde det vara drivande för deras eget arbetssätt. Därmed spelar inte bara personliga preferenser roll, utan även det omgivande klimatet spelar roll för hur systemutvecklare värderar integritet.

Att översätta och tolka de regelverk och principer som finns till tekniska lösningar är ofta utmanande för systemutvecklarna och många önskar tydligare riktlinjer kring vad de förväntas göra samt hur det ska genomföras (Martin, del Alamo & Yelmo, 2014). Dessa tolkningsproblem är inte helt obekanta. Man har tidigare sett liknande problem vid implementeringen av principer för att tillgängliggöra hemsidor, applikationer och system för alla oavsett funktionsnedsättning och personlig förmåga. Problem inom tillgänglighetsanpassning har man kunnat tackla på ett bra sätt och Martin, del Alamo & Yelmo (2014) menar på att liknande åtgärder kan vara effektiva även i detta fall. Gemensamt för integritet och tillgänglighetsanpassning är att de båda tillhör kategorin icke-funktionella krav. Dessutom har integritet och tillgänglighet olika innebörd för olika användare. Då båda attributen involverar individens rättigheter regleras de ofta av landets lagstiftningar.

Martin, del Alamo & Yelmo (2014) går i sin undersökning igenom de metoder som använts för implementering av tillgänglighet med syftet att hitta riktlinjer och metoder som skulle kunna vara gynnsamma för systemutvecklare att arbeta med för att på ett enklare sätt kunna integrera inbäddad integritet vid systemutveckling. I samarbete med mer än 200 personer från olika branscher och med olika bakgrund har man tillsammans och på ett framgångsrikt sätt tagit fram riktlinjer, metoder och verktyg för att på ett enkelt sätt kunna uppnå kraven för tillgänglighet. Att på liknande sätt definiera och översätta principerna kring integritet till konkreta krav för systemutvecklare att följa menar Martin, del Alamo & Yelmo (2014) är en lovande och förhållandevis genomförbar lösning. Utgångspunkterna för att på ett framgångsrikt göra detta anser Martin, del Alamo & Yelmo (2014) vara följande:

- Samla intressenter från olika bakgrund och branscher för att öppet diskutera och gemensamt komma fram till tydliga krav och principer som är lättolkade för systemutvecklare såväl som användare. Systemutvecklare, produkt- och

tjänsteleverantörer, dataskyddsombud, jurister, forskare inom ämnet och slutanvändare bör alla vara aktiva och delta i diskussionerna för bästa resultat.
- Definiera yrkesroller som är nödvändiga samt hur ansvar ska fördelas mellan de involverade.
- Dela upp kraven för integritet i olika lager där varje lager blir mer detaljerat beskrivet i form av tydliga principer som är nödvändiga för att system ska leva upp till de krav som man önskar uppnå gällande integritet. Varje lager ska ge konkreta krav som systemutvecklare förväntas uppnå. Systemutvecklarna ska jobba för att uppnå kriterierna som definieras av observerbara, testbara och mätbara föremål för varje riktlinje. Teknikerna de använder sig av ska på ett pålitligt och enkelt sätt möta framgångskriterierna.
- Ta fram och förse systemutvecklare med en handbok innehållande tekniker och integritetsmönster. Handboken ska kontinuerligt uppdateras. Det ska framgå vem som är bäst lämpad till att utföra de olika stegen för att på ett effektivt och bra sätt kunna använda sig av de rekommenderade teknikerna och uppnå integritetskraven.
- Definiera hur viktiga integritetskraven är i förhållande till framgångsfaktorerna.

2.5 Vanliga brister i systemutvecklares integritetshantering

Den studie som utfördes av Hadar et al. (2018) visade på att det ofta finns en stor tillgång till integritetsrelaterad teknik men att denna allt för sällan utnyttjas. Studien visade också på att det vanligaste sättet att arbeta med integritet i nuläget är att konfigurera den redan existerande arkitekturen som finns istället för att ändra den grundläggande arkitekturen. Alltså verkar systemutvecklare främst använda *privacy-by-policy* och inte *privacy-by-architecture*. Som det diskuterades i det inledande stycket om de olika tillvägagångssätten väljer man alltså det mindre säkra alternativet. Att enbart använda sig av *privacy-by-policy* bör vara enklare då det snarare blir något man lägger till i slutet av processen istället för något som är inbäddat i systemet. Detta skulle kunna vara en förklaring till att det verkar användas i större utsträckning.

Vidare framgick det genom studien att kryptering var både den mest välkända och vanligaste lösningen. Hadar et al. (2018) påpekar dock att en förklarlig anledning till detta är att kryptering även används till många säkerhetsaspekter och att systemutvecklare ofta associerar integritet med säkerhet. Att kunna skilja på begreppen säkerhet och integritet är också en viktig del i integritetsarbetet. Utan att veta skillnaden mellan de två begreppen är det också svårt att leva upp till dem båda. Säkerhet handlar om att skydda data från skadliga hot medan integritet handlar om att använda data på ett ansvarsfullt sätt. Ett annat fynd från studien (Hadar et al., 2018) var att det sker en stor ansvarsförskjutning gällande just integritet. En del systemutvecklare upplever nämligen att det inte är deras ansvar att hantera integritet.

2.6 Privacy Impact Assessment

Privacy Impact Assessment är ett instrument för att skydda integritet. David Wright och Paul De Hert skriver i boken Privacy Impact Assessment (2012, s. 4–10) att bedömningen är mer än bara ett verktyg. De menar att det är en hel process som bör sättas igång så tidigt som möjligt i ett projekt när det fortfarande finns en chans att påverka utkomsten. En väl genomförd Privacy Impact Assessment kommer redan från början engagera olika intressenter

för att kunna samla in deras åsikter och idéer gällande hur inkräktande på personlig integritet kan undvikas eller lindras. Wright & De Hert (2012) påpekar också att detta måste vara en integrerad del av planeringsfasen i projektet för att vara effektivt. Poängen med bedömningen är att identifiera de potentiella effekter som ett projekt kan ha på personlig data för att därefter utreda hur skadliga effekter kan lindras.

Även om det finns flertalet juridiska dokument som beskriver processen för att genomföra en Privacy Impact Assessment menar Ahmadian, Strüber, Riediger & Jürjens (2018) att de i allmänhet inte är lämpliga som referensmodeller. De menar att dessa dokument endast beskriver generiska och abstrakta steg som inte beaktar den konkreta utformningen av ett system. Införandet av Privacy Impact Assessment i IT-sektorn är fortfarande ovanligt, speciellt i Europa, vilket författarna tror kan bero på den tidigare bristen på rättsliga incitament. I sin artikel har författarna ämnat besvara hur konkreta integritetshot kan identifieras och hur en modellbaserad integritetsanalys kan stödja bedömningen för att göra ramverket mer konkret och lättillgängligt. I artikeln skapar författarna just en modellbaserad integritetsanalys som stödjer Privacy Impact Assessment. För att stödja Privacy by Design menar Ahmadian et al. (2018) att metodiken ska appliceras i de tidiga faserna av systemdesignen. Författarna påpekar dock att den också kan användas för att utföra detta på redan existerande system. Alltså är metodiken relativt flexibel och ger även existerande system en chans att förbättra sin integritetshantering.

Modellen skapad av Ahmadian et al. (2018) består av olika steg där det första steget handlar om att skapa en systematisk specifikation av systemet och dess integritetskritiska delar. I det första steget verifierar man också om det är nödvändigt att utföra en Privacy Impact Assessment genom att ställa modellen mot integritets- och säkerhetsprofiler. Sedan görs en analys gällande integritets- och säkerhetskrav. Integritetskontrollerna baseras på fyra nyckelelement: *purpose* (befogade skäl att få tillgång till data), *visibility* (vem som har befogenheten att få tillgång till data), *granularity* (nivån av precision av data) och *retention* (när måste data bli raderad eller begränsad). Därefter identifieras skadliga aktiviteter och hot genom att man utvärderar analysresultaten från föregående steg. Därpå specificeras de identifierade designbristernas påverkan på systemet och en riskbedömning utförs för att kunna identifiera vad som är i riskzonen. Till sist identifieras och rekommenderas lämpliga integritets- och säkerhetskontroller för att lindra riskerna och förbättra systemdesignen.

2.7 Sammanfattning av litteraturgenomgången

I tabell 1 nedan redovisas en sammanfattning av den litteratur som presenterats tillsammans med centrala nyckelord som litteraturen behandlat. Området Privacy by Design i tabellen innefattar även utmaningarna med konceptet.

Tabell 1: Litteratursammanfattning

Område	**Nyckelord**	**Litteraturhänvisning**
Systemutvecklares syn på integritet	Skillnad juridiskt/tekniskt Teoretiskt koncept Osäkerhet	Hadar et al., 2018

	Social aspekt	
Privacy by Design	Vaga principer Teoretiskt Stöd och engagemang Förlorade tjänster Ansvar Utbildning Öppenhet Ökad säkerhet	Cavoukian, 2009 Martin, del Alamo & Yelmo, 2014 Spiekermann, 2012 Schwartz, 2009 Cavoukian, Taylor & Abrams, 2010 Bu et al., 2020
Integritet i systemutvecklingsprocessen	Olika tillvägagångssätt Skydd och säkerhet Organisatoriskt klimat Personliga upplevelser och preferenser Belastning Negativt Kunskapsbrist Tolkningssvårigheter	Hadar et al., 2018 Ayalon et al., 2017 Bu et al., 2020 Martin, del Alamo & Yelmo, 2014
Vanliga brister i systemutvecklares integritetshantering	Outnyttjad teknik *Add-on* lösningar Integritet i förhållande till säkerhet Ansvarsförskjutning	Hadar et al., 2018
Privacy Impact Assessment	Skapa engagemang Tidig integrering Abstrakta steg Riskbedömning	Wright & De Hert, 2012 Ahmadian et al., 2018

3 Metod

Under följande kapitel presenteras valet av metod för utförandet av studien samt hur detta tillämpades. Kapitlet inleds med en förklaring och motivering av metodvalet samt hur valet av organisation och intervjupersoner gick till. Därefter presenteras den specifika metoden vi valt för studien och hur denna utfördes. Vidare tas det upp hur insamlad data bearbetades och analyserades för att avslutningsvis diskutera etik, validitet och reliabilitet.

3.1 Metodval

Efter att ha granskat den befintliga litteraturen inom området hade vi tillräckligt mycket kunskap för att kunna formulera en hypotes om ämnet. Tidigare forskning inom området gav oss intrycket att Privacy by Design ofta är svårt att inkorporera i systemutvecklingsprocessen eftersom det ofta saknas konkreta, tekniska aspekter gällande hur detta bör göras. Allt verkar klart och tydligt i teorin, men när man väl ska omsätta det i praktiken dyker det upp många svårigheter som inte tas upp eller reds ut i teorin. För att undersöka detta vidare utfördes följande empiri.

3.1.1 Kvalitativa studier

Kvalitativ empiri handlar om särskilda kvaliteter och egenskaper hos det som man studerar (Rienecker & Jørgensen, 2014). Vi valde att utföra en kvalitativ metod eftersom vi främst är intresserade av den sociala kontexten i sammanhanget. Studien fokuserar på människor, och då specifikt systemutvecklare, och hur de agerar när det kommer till integritetshantering i systemutvecklingsprocessen. Genom att utföra en kvalitativ metod istället för en kvantitativ kan vi lättare förstå människor och hur de tänker samt få en bredare förståelse för den situation de lever och arbetar i. Vi ansåg att en kvalitativ undersökningsmetod passade vår studie bäst då vi behöver gå in mer på djupet och förstå hur just specifika systemutvecklare ser på och arbetar med integritet. En kvantitativ studie hade inte kunnat ge oss samma insyn i hur de ser på systemutvecklingsprocessen och integritet som en del i detta.

Det bör poängteras att ett problem med kvalitativa studier är att det är en väldigt begränsad mängd observationer. Detta gör såklart att vi inte kan påstå något generellt utifrån observationerna då dem är alldeles för få, men vi kan givetvis uttala oss om det som gäller för just de data vi undersökt (Rienecker & Jørgensen, 2014). Dessutom handlar kvalitativa studier till stor del om att kunna tolka den insamlade datan på rätt sätt. Tolkningen som behöver ske ger utrymme för oetiskt beteende där man, antingen med avsikt eller inte, riskerar att förvrida det personerna sagt till något de inte menade. Med dessa nackdelar i åtanke gick vi vidare i processen till urvalet av organisation och intervjupersoner.

3.2 Urval

I kommande avsnitt beskriver och motiverar vi processen bakom vårt val av organisation samt valet av intervjupersoner inom denna organisation.

3.2.1 Val av organisation

Då vi hade begränsad tid på oss att hitta intervjupersoner gjordes ett bekvämlighetsurval genom kontakter inom området. En av författarna hade ett antal kontakter på olika verksamheter som vi hörde av oss till. Det var både kontakter som själva arbetar som systemutvecklare och personer som inte gör det men som har nära kontakt med andra anställda som är systemutvecklare. För dessa kontakter berättade vi att vi sökte ett antal systemutvecklare som ville ställa upp på en intervju där huvudfokuset var hur de såg på och arbetade med personlig integritet. Vi fick snabbt svar från en kontakt som arbetar på en verksamhet inom den offentliga sektorn. Kontaktpersonen arbetar inte själv som systemutvecklare men hade lyckats samla ihop fem systemutvecklare som gärna ställde upp på intervju.

3.2.2 Val av intervjupersoner

Vi hade inget ytterligare krav på våra intervjupersoner mer än att de skulle arbeta som systemutvecklare. Vår frågeställning är ganska bred då den implicerar att vi hanterar alla systemutvecklare och inte bara exempelvis frontend eller backend-utvecklare. För att följa vår frågeställning och därmed ge läsaren vad denne förväntat sig valde vi att inte begränsa oss gällande någon specifik roll eller specifik typ av systemutvecklare. Eftersom vår kontaktperson på den valda organisationen samlade ihop flertalet systemutvecklare som var villiga att ställa upp på en intervju behövde vi inte själva göra något ytterligare urval. Vi tog sedan kontakt med intervjupersonerna och presenterade oss samt vad vårt mål med intervjun var.

3.3 Intervjuer

Intervjuer är troligtvis den mest använda metoden inom kvalitativ forskning (Bryman, 2016, s. 561). Vi ansåg att intervjuer var den mest aktuella kvalitativa metoden att använda då dessa skulle ge oss möjlighet att styra inriktningen på samtalet samt ge oss en bred och bra uppfattning gällande deras relation till digital integritet i arbetet. För sådana här studier är det viktigt att ha förståelse för hur intervjupersonerna ser på och förstår saker samt att kunna bryta ner deras känslor till något konkret och användbart. För att vi på ett så bra sätt som möjligt ska kunna göra detta kom vi fram till att intervjuer var den bästa metoden för vår studie.

Inför intervjuerna utformades en intervjuguide. Denna innehöll inledande frågor för att ta reda på den specifika systemutvecklarens roll och arbetsuppgifter samt vidare frågor gällande just deras relation till digital integritet. Intervjuerna var semistrukturerade för att erbjuda en viss flexibilitet när det gäller frågornas ordningsföljd och uppföljning av ett svar (Bryman, 2016, s. 581). Ytterligare en motivering till valet av just semistrukturerade intervjuer är att de ofta används när man vill ta sig an specifika frågeställningar (Bryman, 2016, s. 563), vilket vår studie gör. Vi utgick som sagt från vissa grundfrågor för att guida intervjun i rätt riktning och

hjälpa oss att hålla oss till ämnet. Frågorna var till stor grad väldigt öppna, med avsikten att väcka diskussion. Beroende på var diskussionen ledde ställdes olika följdfrågor som ibland tog oss in på andra områden. Genom att kunna följa upp intressanta svar kunde vi på ett bättre sätt få fram komplexiteten och rikedomen i det som studeras (så kallad *rich data*).

3.3.1 Genomförande

Den första intervjun blev mer av en pilotintervju, även om det inte var tanken från början. Efter att ha utfört denna ändrade vi om en del i vår intervjuteknik. Det vi främst märkte var att intervjun blev väldigt kort och ytlig då det var svårt att komma in i några mer djupgående diskussioner. Vi försökte i den mån vi kunde skapa diskussion med intervjupersonen, men upplevde detta ibland som väldigt svårt. Personen hade ofta bestämda åsikter och förklarade kort och koncist varför denne tyckte så. Det blev därmed svårt att föra konversationen vidare. Det är en fin gräns mellan att pusha intervjupersonen till att förklara alla sina tankar och motivera sina åsikter och att vara allt för påträngande. Vi ville inte fråga saker som *"Varför tycker du si och inte så?"* med risk för att personen skulle känna sig ifrågasatt och som att denne tyckte fel. Anledningen att vi såg detta som en tuff balansgång beror till stor del på vår ovana vid att föra intervjuer.

Det vi ändrade i vår intervjuteknik var att vi adderade en del reservfrågor som kunde vara av intresse att prata vidare kring ifall vi inte lyckades skapa någon vidare diskussion (se Bilaga 1 för fullständig intervjuguide). I de efterföljande intervjuerna upplevde vi att den nämnda svårigheten blev mindre och mindre, antagligen för att vi också blev mer vana vid konceptet och inte längre lika överväldigade av all information. Intervjupersonerna var väldigt olika och en del pratade gladeligen på medan andra var mer fokuserade på att enbart besvara våra frågor och gav väldigt korta svar vid eventuella följdfrågor. Därav använde vi ibland alla, ibland en del och ibland inga alls av reservfrågorna. Vi upplevde även att intervjuerna blev bättre och mer djupgående efter omarbetningen av frågorna.

Alla intervjuer hölls på distans via Zoom. Anledningen till att vi valde Zoom som mötestjänst var för att det är den tjänst vi använt via skolan och därmed är vana vid. Självklart hade vi föredragit att möta intervjupersonerna på riktigt, ansikte mot ansikte. Detta var inte möjligt på grund av rådande pandemi och eftersom de flesta ändå arbetade hemifrån ansåg vi att en tjänst som Zoom var bättre än till exempel ett telefonsamtal. Tanken var att intervjupersonerna då fick ett ansikte på oss som intervjuade och att de då skulle känna sig mer bekväma. Vår förhoppning var också att på grund av att intervjun skedde hemifrån kände sig intervjupersonerna inte begränsade i att uttrycka vad de egentligen tyckte och tänkte med risk för att någon kollega skulle överhöra det de sade eller liknande.

Under intervjuernas gång hade författarna olika ansvarsuppgifter. Den författare som bjudit in till Zoom-mötet var även den som såg till att påbörja och avsluta inspelningen av intervjun. Den andra författaren hade i sin tur som uppgift att dela skärm när det var dags att visa två olika scenarier som intervjupersonerna skulle ta ställning till. Detta gjordes för att scenarierna var långa med mycket information att ta hänsyn till och hade hela fem olika svarsalternativ. Genom att dela skärm kunde intervjupersonerna läsa scenariot i sin egen takt och sedan ta sin tid att fundera på sitt svar samtidigt som de hade scenariot och svaren framför sig. När det kom till frågeställandet fanns ingen specifik uppdelning utan det delades ungefär lika mellan de båda författarna.

Tabell 2: Respondenter och intervjudetaljer

Respondent	Utvecklarroll	Typ av intervju	Längd på intervju	Inspelad
R1	Frontend	Zoom	16 min	Ja
R2	Fullstack	Zoom	23 min	Ja
R3	Fullstack	Zoom	15 min	Ja
R4	Fullstack	Zoom	32 min	Ja
R5	Fullstack	Zoom	20 min	Ja

3.3.2 Intervjuernas uppbyggnad

Intervjuerna bestod av sex olika delar där de två första var mer inledande och generella. Därefter gick vi allt djupare in på ämnet för varje del för att på så sätt komma närmre och närmre våra forskningsfrågor. I tabell 3 beskrivs de olika delarna på ett övergripande sätt.

Tabell 3: Intervjuguide

Introduktion	Presentation av oss, syftet med vår studie och vad vi främst var intresserade av. Detta gjordes för att säkerställa att intervjupersonerna fick en tydlig bild av syftet med intervjun, för att därigenom ge oss så bra svar som möjligt. Vi nämnde också att vi läst på om ämnet för att inge förtroende genom att visa att vi har mycket kunskap inom området. Intervjupersonen tillfrågades även om denne var okej med att intervjun spelades in.
Uppvärmningsfrågor	Frågor om vilken roll personen har, vad den arbetar med samt vad detta innebär för aktiviteter. Detta gjordes dels för att få en bättre bild av den kontext denne arbetar i men också för att börja intervjun på ett mer avslappnat sätt.
Syn på integritet	Början på intervjuns huvuddel. Frågor om hur personen ser på digital integritet och om de upplever att det finns i deras arbete. Utreder om det finns en osäkerhet kopplat till begreppet och hur den sociala aspekten spelar in. Svaren på dessa inledande frågor gav oss en fingervisning om hur personens

	förhållande till integritet var och utifrån detta ställde vi andra relevanta frågor.
Integritet i systemutvecklingsprocessen	Huruvida de känner till Privacy by Design och i så fall i vilken mån detta återfinns som en strategi i deras arbete. Om de arbetar/har arbetat med integritet i systemutvecklingsprocessen fick de förklara sina tillvägagångssätt och svara på om det upplevts som en ökad belastning.
Scenarioanalys	Största delen som fungerade som underlag för diskussion. Personen fick läsa två scenarier och sen ta ställning till olika alternativ utifrån vad som hade passat deras agerande bäst. Detta tvingade personerna sätta sig in i faktiska problematiska situationer och sedan tänka högt hur de hade löst dem. Det gav oss en insikt i deras personliga upplevelser och preferenser samt eventuell ansvarsförskjutning.
Avslutning	För att markera slutet av intervjun berättade vi att det var alla frågor vi hade och att vi kände att vi hade täckt alla tänkta områden. Vi påpekade att det hade varit väldigt lärorikt och tackade för deras medverkan.

3.4 Bearbetning av data

Efter att en intervju var avslutad påbörjade vi arbetet med att transkribera. Med hjälp av transkriberingen av intervjuerna blev det sedan enklare att gå tillbaka till specifika delar av intervjuerna vilket var ytterst hjälpsamt vid analysen av datan. Genom att ha intervjuerna i textformat var det också enkelt att få en snabb överblick av det som hade sagts. Att spela in intervjuer för att senare transkriberas tillåter också frågeställarna fokusera mer på de svar som ges genom att inte bli distraherade av att föra anteckningar (Bryman, 2016, s. 278). Genom att transkribera efterhand och inte vänta tills alla intervjuer var avklarade påbörjades på så sätt analysen av materialet tidigt i processen. Genom denna kontinuerliga process blev vi mer medvetna om olika mönster som förekom (Bryman, 2016, s. 279) och kunde därifrån hämta intressanta ämnen att ta upp på de återstående intervjuerna.

För att utröna vad i intervjuerna som var relevant för vår studie bestämde vi oss för att koda intervjuerna efter de olika områdena som listades i tabell 1, med viss modifikation. Den främsta förändringen var att de två sista rubrikerna *Vanliga brister i utvecklares integritetshantering* och *Privacy Impact Assessment* inte togs med då dessa områden inte diskuterades i intervjuerna. Genom att koda intervjuerna blev det mycket enklare att föra över relevant information till empirin på ett strukturerat sätt. Den struktur som skapades med hjälp

av kodningen gjorde att empirin senare lätt kunde jämföras med litteraturgenomgången. Kodningen delades upp i följande kategorier:

Tabell 4: Kodöversikt

Kod	Kategori
SI-U	Systemutvecklares syn på integritet, som utvecklare
SI-A	Systemutvecklares syn på integritet, som användare
PbD-B	Bekantskap med begreppet Privacy By Design
PbD-U	Utmaningar kopplade till Privacy by Design/integritet
PbD-T	Användning av ny teknologi
IP	Integritet i systemutvecklingsprocessen generellt
IP-M	Metoder för att identifiera olika risker eller designval
IP-NP	Normer och policies för integritetshantering
C1	Första scenarioanalysen
C2	Andra scenarioanalysen

3.5 Validitet, reliabilitet och etik

3.5.1 Etik

För att både forskarna och deltagarna i studien ska känna sig trygga bör vissa etiska principer följas vid forskningsarbete. Dessa är bland annat (Recker, 2013):

- Studien får inte orsaka onödig skada. Studien får alltså inte bidra till fysisk eller psykologisk stress eller skada för deltagarna.
- Forskarna måste försäkra sig om att de har medgivande från deltagarna att utföra intervjun.
- Deltagarna ska ha rätt till anonymitet om så önskas.
- Sekretess måste vidhållas.

För att på bästa sätt följa principerna och skapa trygghet för alla deltagande valde vi att genomföra vissa aktiviteter på ett specifikt sätt. Den första kontakten med intervjupersonerna skedde till exempel via mejl med tanken att personerna då skulle ha lättare för att säga nej om de inte hade tid eller hade ångrat sig. Detta för att det ofta är lättare att avböja något skriftligt

än i tal. Vi hade tidigare hört av oss till en kontakt som informerat intervjupersonerna om vår forskning och undersökt intresset för deltagande. Efter detta hörde vi av oss till intervjupersonerna, presenterade oss samt introducerade vår forskning kortfattat. Genom att presentera vår forskning har deltagarna på ett informerat sätt kunna ta ställning till sin medverkan. Samtliga deltagare tackade skriftligen ja till medverkandet och informerades om att deras identiteter skulle förbli anonyma. Detta för att de skulle känna sig trygga och ge ärliga svar.

Då intervjun genomfördes på distans via Zoom såg vi möjligheten till att spela in intervjun för att senare kunna transkribera materialet. Vi frågade deltagarna om detta var okej samt försäkrade dem vid förfrågan om att materialet enbart skulle användas av oss och i syfte för studien. Samtliga deltagare gav samtycke till inspelningen av samtalet. För att säkerställa att etiska principer vidhållits och att alla intervjupersonerna kände att deras åsikter speglats på ett korrekt sätt skickades empirin ut till intervjupersonerna när denna var klar. Samtliga godkände empirin via mejl. Inspelningen av intervjuerna raderades också när transkriberingen var färdigställd för att vidhålla hög grad av anonymitet.

3.5.2 Validitet

Validitet handlar om hur man mäter det man säger sig mäta (Bryman, 2016, s. 465). För att hålla hög intern validitet i studien är det viktigt att det finns en god överensstämmelse mellan vad intervjupersonerna menade med sitt svar och forskarens tolkning av svaret (Bryman, 2016, s. 465). Detta har vi säkerställt genom att skicka ut empirin till intervjupersonerna för godkännande. Dessutom var det behjälpligt att vi använde oss av semistrukturerade intervjuer då dessa också lämnade utrymme för vidare förklaring, vilket minskade risken för feltolkning. Extern validitet är dock svårare att uppnå för kvalitativa studier då de ofta grundar sig på ett begränsat urval (LeCompte & Goetz, 1982). Det blir därmed svårt att generalisera kvalitativa studier till andra situationer och miljöer (Bryman, 2016, s. 466). Den externa validiteten i vår studie är låg, speciellt eftersom vi har ett så begränsat urval med enbart en organisation i den offentliga sektorn. För att öka validiteten något hade vi kunnat intervjua systemutvecklare från flera olika organisationer inom både den privata och offentliga sektorn.

3.5.3 Reliabilitet

Reliabilitet beskriver hur tillförlitligt någonting är (Nationalencyklopedin, n.d. b). Ett exempel på hög reliabilitet är när flera olika forskningsstudier oberoende av varandra kan dra samma slutsatser. Extern reliabilitet avser i vilken utsträckning en undersökning kan replikeras (LeCompte & Goetz, 1982). Det är ofta svårt att uppnå hög extern reliabilitet inom kvalitativ forskning eftersom det aldrig går att replikera en social kontext helt och hållet. Studien bygger även på semistrukturerade intervjuer där samtalet till stor del styrs av intervjupersonens svar vilket även det försvårar ett eventuellt återskapande av studien. Studiens tillvägagångssätt finns dock beskrivet i detalj i intervjuguiden (se Bilaga 1) och metodavsnittet vilket kan stärka den externa reliabiliteten något. Intern reliabilitet handlar i sin tur om att medlemmarna i ett forskarlag är överens om hur den insamlade datan ska tolkas (LeCompte & Goetz, 1982). Vi har försökt vidhålla hög intern reliabilitet genom att vi skapade passande koder att dela in datan i samt gick igenom och analyserade därefter datan tillsammans.

3.6 Metodreflektion

Med hänsyn till ovanstående kapitel om validitet och reliabilitet har vi kritiskt granskat vår metod för att uppmärksamma vissa brister som bör tas i beaktning vid en eventuell ny studie. Som vi nämnde i avsnittet om validitet hade studien kunnat dra mer generella slutsatser om vi haft ett bredare underlag för intervjuerna. Genom att undersöka både den privata och offentliga sektorn hade vi kunnat jämföra dessa och därmed även avgöra om attityden till integritet skiljer sig mellan de olika sektorerna. Man kan även tänka sig att vi i alla fall borde ha intervjuat systemutvecklare från flera olika verksamheter inom den offentliga sektorn för att göra vår studie något bredare. Vi menar dock att vi hellre intervjuar flera personer från samma organisation än flera personer från varsin organisation. Eftersom det organisatoriska klimatet ofta togs upp som en bidragande faktor till attityden till integritet ville vi undersöka detta, vilket hade varit svårt om alla varit från olika organisationer. Detta eftersom det är svårt att få en korrekt bild av det organisatoriska klimatet genom enbart en intervjuperson.

Vi vill poängtera att det också är viktigt att ta hänsyn till studiens omfång och på ett realistiskt sätt inse att vi inte hade haft tid att genomföra så många intervjuer som en undersökning av både privat och offentlig sektor, eller flertalet verksamheter inom den offentliga sektorn, hade krävt. Om vi skulle ha gjort om studien hade vi valt att enbart fokusera på en eller två kommersiella verksamheter. Begränsningen av antalet organisationer motiveras med det som beskrevs ovan. Anledningen av skiftet från offentlig till privat sektor är för att de inom den privata sektorn har större anledning att försöka kringgå visst integritetsskydd då de tjänar pengar på insamlad data genom exempelvis reklamintäkter som ofta baseras på personlig data (Spiekermann, 2012). Därmed tror vi att den här typen av organisationer kan bli mer intressanta att undersöka.

4 Empiri

I följande kapitel sammanställs resultatet av de genomförda intervjuerna. Vid analysen av all insamlad data har ett urval gjorts där enbart svar som på något sätt är relevanta för våra forskningsfrågor tagits med. Långa, utläggande svar har också kortats ner till deras kärnpunkter. Detta resulterar i att de inledande frågorna om personens roll inte har tagits med. Det bör också noteras att det inte finns något svar från R1 på vissa områden då en del områden tillkom efter revideringen av frågorna. Dessutom blev inte alla intervjupersoner tillfrågade om exakt samma ämnen då frågorna till stor del berodde på deras tidigare svar. Därför saknas ibland vissa intervjupersoner under vissa underrubriker. Både intervjupersonerna och organisationen har anonymiserats. Intervjupersonerna nämns istället som respondenter (R1-R5) och organisationen omnämns som Organisationen.

4.1 Systemutvecklares syn på integritet

4.1.1 Som systemutvecklare

Åsikterna kring integritet inom arbetet varierade bland deltagarna i studien. En del ansåg att de inte behövde tänka på det inom sin arbetsroll medan andra tyckte det var något som ingick i arbetet och var svårhanterat. R1 uppfattade integritet inom frontend-utveckling som något svårnavigerat. Att lagar som införts helt klart försvårat arbetet var något som betonades under intervjun. R2 har jobbat mycket med känslig data i sin roll och är mån om att hantera det på ett korrekt sätt. Under arbetet försöker personen resonera kring vad som bör undvikas och hur man ska tänka för att säkerställa att användares personliga integritet bibehålls. En allmän försiktighet är vad som ligger till grund för hur R2 tänker kring hantering och bevarandet av användarnas integritet. R3 berättade att personen gått på en del kurser gällande digital integritet och att vikten av det även togs upp under personens studietid men att kunskapen inte har behövt användas så mycket i arbetet på Organisationen. Därmed hade personen inte någon speciell syn på integritet i arbetslivet. Däremot var R3 glad över att det inte behövdes i arbetet då personen ansåg det vara psykiskt påfrestande.

Att tänka på hur man agerar, hanterar data och inte kränker andras personliga integritet anser R4 vara något man får göra som systemutvecklare. Att följa lagstiftningarna som finns är viktigt men anses vara lite av en djungel där det är svårt att förstå om man gör rätt eller fel och det blir då problematiskt att implementera i praktiken. På frågan om hur man ser på personlig integritet i allmänhet svarade R5 kort: *”Alltså jag har ju inte funderat så mycket på det.”*. R5 berättade att personen inte tänkt så mycket på personlig integritet ur ett utvecklarperspektiv heller men betonade att man inte kan komplicera system hur mycket som helst enbart för att användare kanske inte vill uppge information om något. Man behöver inte samla in data om den inte är relevant men personen menar samtidigt på att man måste kunna jobba på ett smidigt sätt och att det då kan krävas att användaren offrar en del av sin integritet.

4.1.2 Som användare

Gemensamt för alla intervjupersoner var att alla mer eller mindre var medvetna om att integriteten i dagens teknologier var begränsad. Huruvida detta var ett problem eller inte varierade mellan deltagarna. R1 menade att de lagar och riktlinjer som finns idag för att skydda privatpersoner inom den digitala världen är bra och fortsatte med *"...det gör även mitt användande av internet som privatperson jävligt mycket roligare."*. Personen ansåg att dessa bidrog till ett roligare och tryggare användande av internet. R2 visade på mer oro gällande integritet i privatlivet och tog upp hur det idag finns många system som kan mycket om många individer. Ett exempel som togs upp var ett scenario i USA där man kunde få inreseförbud till landet baserat på vad man delat med sig av på sociala medier. Om innehållet klassas som olämpligt kan beslut tas om att inte släppa in personen i landet. R2 tyckte detta var en obehaglig utveckling och att det kan vara problematiskt att så enkelt kunna hitta information om alla på en global nivå. Personen tyckte att man bör vara medveten om att det finns mycket lättillgänglig information om en.

Under sina universitetsstudier läste R3 lite om personlig integritet i samband med systemutveckling men det är inget personen reflekterar kring så mycket. Personen anser sig själv ha samma syn på ämnet både yrkesmässigt och privat. R4 håller med R2 om att integriteten på nätet inte är särskilt stor men att det är något viktigt. R4 tog upp att det är ett svårt ämne där man i så fall själv får jobba aktivt med att skydda sig och tog upp ett exempel om att *"I stort sett allt du gör ser Google liksom, Google vet säkert mer om mig än vad jag vet."*. R4 anser inte sig själv vara manisk gällande ämnet. Tankarna finns där och det är inget personen gillar men får acceptera då R4 vill kunna använda sig av gratistjänster som Facebook, Gmail och liknande.

R5 berättar att personen inte funderat på det så mycket och har lite av en obrydd inställning gentemot ämnet men att tankarna varit lite fler nu i samband med Apples nya uppdatering som ger användaren möjlighet till att stoppa appspårning. Personen gör en jämförelse mellan ämnet och det svenska personnumret och menar att systemet med personnumret redan gör att svenska folket ligger illa till ur ett integritetsperspektiv. Personnummer räknas som offentlig handling och säger väldigt mycket om varje individ. Personen menar att om man visar sitt personnummer har man redan sagt ganska mycket om sig själv. R5 menar att om man vill ta del av vissa tjänster måste man offra lite och det får man helt enkelt försöka acceptera.

Tabell 5: Sammanfattning av systemutvecklarnas syn på integritet

Respondent	Systemutvecklarperspektiv	Användarperspektiv
R1	Svårnavigerat område som försvårat arbetet en del.	Ser positivt på och är nöjd med de regleringar som finns för att skydda integritet.
R2	Viktigt ämne, vidtar därför alltid en allmän försiktighet.	Uttrycker viss oro över bristen på integritet, anser att det fått en obehaglig utveckling.
R3	Anser sig inte arbeta med det och upplever detta som skönt.	Ingen speciell åsikt. Säger sig ha samma synsätt privat som i arbetslivet.
R4	Viktigt ämne, anser att det är en del av arbetet som systemutvecklare.	Gillar inte inkräktandet på integritet som ofta sker, men vidtar inga åtgärder för att skydda sig mot detta.
R5	Har inte tänkt på det så mycket.	Ganska obrydd generellt, anser att vill man vara en del av de tjänster som finns får man också vara beredd att offra en del av sin integritet.

4.2 Privacy by Design

4.2.1 Bekantskap med begreppet Privacy by Design

Av de tillfrågade verkade de flesta ha hört begreppet förut, men inte mycket mer än så. R3 kände till begreppet sedan tidigare, men visste inte riktigt vad det innebar. Som svar på frågan i vilken mån R2 kände till begreppet svarade personen: *"För mig såg jag det som att det var svårt att tillämpa det i praktiken på vårt arbete. Att jag liksom därför sorterade bort och inte gick vidare, men inte mer än så."*. R4 hade inte hört just Privacy by Design men gissade sig till vad det innebar och förstod tanken med själva konceptet. Alla tillfrågade intervjupersoner svarade också att detta inte var något de använde i sitt arbete. R4 påpekade att de flesta projekt de utför inte är att bygga nya system utan snarare att uppdatera och utveckla redan existerande system. Detta kan vara en förklaring till den blygsamma kännedomen till begreppet. Vidare förklarade R5 också att eftersom Organisationen är en verksamhet inom den offentliga sektorn slipper de ganska mycket av det bry och arbete med integritet som kommersiella företag råkar ut för.

4.2.2 Utmaningar kopplade till integritet

R1 poängterade att det är svårt att veta vad GDPR egentligen innebär och att de flesta bara vet om att det är något man måste anpassa sig till. På frågan om varför GDPR upplevs som otydligt eller svårtolkat svarade personen att *"...det kom väldigt hårda krav på att vi skulle GDPR-anpassa alltihopa men vi fick aldrig tid att lära oss vad GDPR innebar."*. R1 anser också att funktionaliteten har fått kompromissas kraftigt som bekostnad för att följa GDPR, men hade trots det inte velat ändra på detta om möjligheten funnits. Personen motiverar detta med att även om de lagar och regleringar som finns gör jobbet drygare så gör det användandet av internet som privatperson mycket bättre vilket väger tyngre än den eventuellt ökade arbetsbelastningen.

Både R2 och R4 pekade också ut svårigheter att efterleva GDPR och de regelverk som finns, främst på grund av att de är svåra att omsätta i praktiken. R2 gav som exempel att de ibland rådfrågar jurister när det finns oklarheter men att juristerna ofta är väldigt försiktiga med att uttala sig och att de är så pass försiktiga att det inte går att arbeta efter. R2 tror att den främsta anledningen till denna försiktighetsprincip är att det inte finns några prejudikat, alltså inga rättsfall som prövats inom GDPR eller integritet. R2 svarade även att det kan finnas brister i juristers förståelse för de tekniska delarna och reflekterade även självkritiskt om att *"Vi kanske inte heller alltid är så duktiga på att kommunicera frågeställningen på ett korrekt sätt"*.

R4 diskuterar på ett liknande sätt att det knappast finns en brist på olika ramverk och lagstiftningar utan att de snarare är svåra att översätta till en teknisk, mer detaljerad nivå. Vid frågan om vad som skulle kunna förbättras svarar R4 att det hade varit bra med konkreta exempel på vad som är tillåtet och inte. När vi tar upp den juridiska biten håller personen med om R2s påstående. Vidare tar R4 upp ett intressant fall, nämligen Schrems-domen, som är en dom som kom sommaren 2020 och som innebar att man inte längre får föra över personlig data till USA. R4 menar att detta då blir ännu en svårighet att förhålla sig till då man inte säkert vet vad som gäller.

Även cookies är ett snårigt område. R4 ger Organisationens egen hemsida som exempel där olika redaktörer bäddar in material från tjänster som YouTube och Google som i sin tur ger cookies och liknande. Där är gränsen väldigt suddig för vem det är som egentligen har ansvar för dessa. Personen nämner också, precis som R1, att det nog i många av de områden där GDPR hanteras är väldigt få som faktiskt vet hur man ska hantera detta. R4 berättar även att personen varit på utbildningar inom ämnet men intrycket har även där varit att man inte riktigt vet vad som ska göras för att säkerställa att integritetshanteringen utförs på ett korrekt sätt. I nuläget är tveksamheterna många men personen var optimistisk till att det skulle bli tydligare i framtiden. Även R1 tar upp utbildning och att man vid tillfällen tagit in experter som sagt att saker varit bra eller mindre bra men återigen lades inga resurser på att lära medarbetarna hur man skulle arbeta eller varför man gör som man gör.

Precis som föregående intervjupersoner upplever R5 att det kan vara svårt att följa GDPR. Personen poängterar främst att alla tolkar riktlinjerna olika. En del tycker det är acceptabelt att göra vissa saker medan andra inte håller med. Vidare berättar personen att de på Organisationen haft genomgångar om hur man ska gå tillväga men att folk fortfarande tolkar riktlinjerna olika. En önskan var därför att riktlinjerna hade varit lite tydligare. R5 föreslår vidare att någon utvecklare som är intresserad av ämnet skulle behöva reda ut riktlinjerna för att på så sätt göra dem mer omfattande. Efter följer citatet: *"För man kan ju säkert lägga hur*

mycket tid och energi som helst på detta, men det är inte säkert att våra kunder vill betala för det heller till exempel.”.

4.2.3 Användning av ny teknologi

På frågan om Organisationen försöker hålla sig uppdaterade kring ny teknologi inom integritetsområdet svarade alla tillfrågade att de alltid försöker hålla sig uppdaterade kring ny teknik generellt men inte just specifikt gällande integritet. R2 gav som exempel att de alltid ser till att använda saker som ny kryptering, nya certifikat, långa och säkra lösenord o.s.v. R4 svarar på ett liknande sätt att de alltid försöker hitta, läsa på om och använda den senaste teknologin och betonar att det är något man måste göra konstant som utvecklare. Vidare svarar R4 att de inte riktar sig specifikt mot integritet i det här sökandet, men att det per automatik ofta följer med när man håller sig uppdaterad inom systemutveckling generellt. R5 ansåg inte heller att de aktivt höll sig uppdaterade med de senaste teknologierna gällande just integritet utan svarade att *“Vi är nog ganska obrydda tills någon gnäller på oss eller om någon ställer en aktiv fråga just om GDPR till exempel.”.*

Tabell 6: Sammanfattning av Privacy by Design

Respondent	**Begreppet Privacy by Design**	**Utmaningar**	**Ny integritetsteknologi**
R1	Ej tillfrågad.	Svårt att veta vad GDPR innebär. Funktionalitet har fått kompromissas. Utbildningar har inte förklarat varför man ska arbeta som man gör.	Ej tillfrågad.
R2	Hört talas om, men bedömde att det var svårt att omsätta i praktiken och lade därför inte mer energi på det.	Svårt att omsätta GDPR i praktiken. Försiktigheter från den juridiska sidan p.g.a. avsaknaden av prejudikat.	Inte specifikt gällande integritet, men använder ny kryptering, nya certifikat och liknande.
R3	Känner till men vet inte riktigt vad det innebär.	Ej tillfrågad.	Ej tillfrågad.
R4	Inte hört just detta, men kunde gissa vad konceptet gick ut på.	Svårt att omsätta GDPR i praktiken. Försiktigheter från den juridiska sidan	Inte specifikt gällande integritet, men den typen av teknologier följer med när man håller sig uppdaterad inom

		p.g.a. avsaknaden av prejudikat. Oklar ansvarsfördelning vid integrering av tredjepartsapplikationer. De som håller i utbildningar verkar inte heller veta vad man ska göra.	området rent generellt.
R5	Känner inte till.	Svårt att följa GDPR. Alla tolkar riktlinjerna olika trots utbildning.	Inte specifikt gällande integritet.

4.3 Integritet i systemutvecklingsprocessen

R5 och R3 är enade om att de inte råkar ut för så mycket personlig integritetshantering och menar på att när de hanterar system som i sin tur hanterar personlig data så sparas bara den data som anses nödvändig. Det behövs därmed ingen fundering eller diskussion kring den data som sparas eftersom den sparas av en anledning. Organisationen är en verksamhet inom den offentliga sektorn och inget kommersiellt företag och därför sparas ingenting för annat syfte än att det behövs för att systemet ska fungera menar R5. Däremot anser R2 att i deras organisation är det *"...mycket persondata som skiftas runt omkring och det kan vara data som också kan vara känslig."*. Därför är personen mån om hur data behandlas och hur man ska resonera med sig själv för att få en bra och säker process. R2 ger medicinsk data som ett exempel på känslig information. Många gånger kan det vara enklare att arbeta med riktig data istället för att generera testdata, men det kan vara en säkerhetsrisk och är lätt hänt att data hamnar i någon testmiljö och sparas i en äldre kopia.

R1 hanterar en del integritet i sin roll. Framför allt handlar det om antalet cookies och hur de används. Personen berättar att *"...vi gick från 12–13 cookies i snitt per användare till 1 som hade typ 5 minuters livstid. Så det gjorde så att all cachning och all inloggningsinformation blev fruktansvärt mycket mer svårhanterad."*. Att inte kunna använda sig av cookies på samma sätt som tidigare har gjort systemutvecklingen mer utmanande. Att inte kunna spåra användarens aktivitet inom systemen har påverkat effektiviteten och produktiviteten. Man fick i stället komma på andra sätt att tackla det vilket resulterade i att man mer eller mindre fick designa om de delarna i systemet som använde sig av cookies. Detta gjorde att användningstiden och uppladdningstiden tredubblades. I nuläget använder man sig av en cookie som direkt frågar användaren om man är okej med cookies. Personen känner att trots

att det gått en tid sen GDPR infördes har de inte fått någon riktig struktur på hur man arbetar med det.

R4 hanterar en del personuppgifter på webben men inte så mycket som faller under kategorin känsliga personuppgifter. Mestadels handlar det om namn och mejladresser men även personnummer vilket är mer känsligt. Då personen främst jobbar med den externa webben är det viktigt att man är noga med att sortera bort känslig data då all annan data de jobbar med kommer visas utåt. Personen berättar att det finns en annan webbtjänst som hanterar persondata och som i sin tur interagerar med den tjänsten teamet arbetar med. Där får man vara observant på att man inte tar ut personnummer eller annan data som inte anses vara nödvändig.

4.3.1 Metoder för att identifiera olika risker eller designval

R2 berättar att man tidigare haft tillfällen då man kört test suites för att kunna identifiera säkerhetsproblem. Utöver det brukar man försöka hålla saker uppdaterade och inte använda allt för gamla tekniker i systemen *"Då får man ju skyddet någonstans inbyggt. Vi är ju mer oroliga för ett gammalt system som bygger på gamla servrar till exempel och där kanske vi tittar en extra gång…"* förklarar personen. Utöver detta har man också en säkerhetsansvarig som håller utkik efter ovanlig trafik. R2 berättar också om en relativt ny implementerad rutin som går ut på att man letar efter tillfällen där information hade kunnat läcka ut som man då rapporterar vidare och hanterar enligt vissa rutiner. De exakta rutinerna för detta vet inte personen. Till skillnad från R2 så svarade R3 att de inte har några etablerade metoder för hur de ska identifiera olika risker eller designval vilket beror på att personen inte arbetar med system som rör den personliga integriteten. Den data som används är nödvändig och där finns då inte så mycket utrymme till att reflektera kring det. Även R5 håller med och svarade att de inte har några metoder för detta.

4.3.2 Normer och policies för integritetshantering

Som tidigare nämnt så ingår det inte så mycket integritet i R3s roll. Därför nämns inga specifika normer eller principer under intervjun. De system personen arbetar med har oftast gåtts igenom av andra där integritetshanteringen kontrollerats men generellt så brukar de tänka på att försöka hindra exponeringen av personlig data om den inte är nödvändig för systemet. R4 berättar att de ska förhålla sig till den lagstiftning som finns med GDPR och användningen av cookies. Utöver det har de inga egna policies internt på Organisationen. Däremot känner personen ett behov av att kunna vara mer säker på att arbetet görs rätt, förutom det tror inte personen att andra policies hade gett mer stöd utan att man kommer ganska långt genom att följa GDPR. R4 tar upp att de förtydligandena som personen önskar inte är något som de inom Organisationen kan ta fram utan att det måste komma högre uppifrån. Även R5 berättar att de inte har några speciella policies mer än att se till att de lever upp till lagstiftningarna för GDPR. De försöker tänka igenom valen som görs kring data när de utvecklar nya system, och tänker på att inte använda sig av mer data än nödvändigt.

Tabell 7: Sammanfattning av integritet i systemutvecklingsprocessen

Respondent	**Generellt**	**Identifiera risker**	**Normer och policies**
R1	Cookies har blivit mer svårhanterat; effektiviteten och produktiviteten har minskat för systemutvecklarna och användnings- och uppladdningstiden har ökat för användarna. Saknas struktur på hur man arbetar med integritet.	Ej tillfrågad.	Ej tillfrågad.
R2	Anser att Organisationen hanterar mycket persondata.	Man försöker hålla saker uppdaterade. Finns även en rutin som går ut på att leta efter tillfällen där information hade kunnat läcka ut som rapporteras vidare och hanteras enligt vissa rutiner. Finns också en säkerhetsansvarig.	Ej tillfrågad.
R3	Anser inte att Organisationen hanterar så mycket persondata, men om detta görs är det för att det är nödvändigt.	Anser att det inte finns etablerade metoder för hur de ska identifiera olika risker eller designval.	Finns inga etablerade normer eller policies, men man försöker tänka på att hindra exponeringen av personlig data om den inte är absolut nödvändig.
R4	Anser sig inte hantera så mycket känsliga personuppgifter.	Ej tillfrågad.	Finns inga etablerade normer eller policies förutom att förhålla sig till GDPR och

			användningen av cookies.
R5	Anser inte att Organisationen hanterar så mycket persondata, men om detta görs är det för att det är nödvändigt.	Finns ingen etablerad metod för detta.	Finns inga etablerade normer eller policies förutom att förhålla sig till GDPR och att inte använda sig av mer data än nödvändigt.

4.4 Scenarioanalys

4.4.1 Scenario 1

Följande scenario är direkt taget och översatt från Bu et al. (2020):

"Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. I projektet finns det en väldigt tydlig arbetsfördelning gällande inloggningsautentisering, verifiering vid betalning, affärsfunktioner etc. Tom är ansvarig för utvecklingen av några affärsfunktioner gällande användare, skapandet av ett användargränssnitt samt kopplingen mellan frontend och backend. Om du var Tom, vilket av de följande alternativen stämmer bäst överens med din åsikt?

A. Mitt arbete involverar inte extern dataöverföring. Integritets- och säkerhetsrelaterade problem är inte en del av min uppgift, ansvaret borde ligga på de som testar säkerheten.
B. Att prestera på arbetet är viktigt för mig och jag borde slutföra mitt arbete så snart som möjligt. Integritets- och säkerhetsskydd är inte en kritisk fråga som jag behöver beakta.
C. Jag kommer slutföra mitt arbete så snart som möjligt. Jag kommer testa huruvida det finns en risk för integritetsintrång efter att alla funktionella krav är uppnådda.
D. Jag kommer beakta huruvida det finns risk för en integritetsläcka kopplat till det jag arbetar med och skapa en integritetsskyddande strategi. Sedan kommer jag slutföra mitt jobb så fort som möjligt.
E. Jag kommer diskutera den integritetsskyddande strategin med alla involverade för att sedan fortsätta med utvecklingen och implementeringen av den framlagda strategin."

Det första scenariot handlar alltså om ansvarstagande och går ut på att ta ställning till huruvida man har ansvar för integritetshantering eller inte och i så fall hur mycket kraft man skulle ha lagt på hanteringen. R1 valde alternativ C som var att man slutförde arbetet med alla funktionella krav först för att efteråt testa om det finns en möjlighet för integritetsintrång. Personen valde detta alternativ eftersom det är så denne arbetar; man bygger först och testar sen om något har gått fel eller inte. Personen nämnde också även att testningen inte skulle vara något av hög prioritet då andra saker som funktionalitet går före. R1 motiverade

ytterligare sitt svar med att påpeka att funktionaliteten är det som är svårt att få till bra och att denne därför alltid börjar med detta.

Både R2 och R3 valde i sin tur alternativ E som var alternativet med den mest ansvarstagande åtgärden. Där innebar svaret att man skulle utveckla och implementera en integritetsskyddande strategi tillsammans med alla involverade. R2 motiverade sitt val med att det var på så sätt som denne agerat i liknande situationer tidigare. R3 som valde samma alternativ motiverar detta med att det inte är ett beslut som ska tas själv utan som behöver diskuteras med andra som är involverade. Personen ansåg det också vara viktigt att ha en fastställd strategi för hur man ska angripa frågan innan man kommer allt för långt i systemutvecklingsprocessen för att *"Beroende på hur man väljer att angripa det så kommer ju lösningarna till att se väldigt olika ut. Så det är någonting man måste ha med redan från början."*.

Både R4 och R5 funderade länge på sina svar och velade mellan svarsalternativ D och E. Alternativ D liknar alternativ E väldigt mycket med den enda skillnaden att i alternativ D diskuteras inte frågan med några andra. R4 ansåg att ansvarsområdet var så känsligt det kan bli gällande just integritet och att man därför måste agera på ett lämpligt sätt. Svaret från R4 blev därför att personen helst av allt hade velat göra alternativ E, men beroende på hur bråttom man har skulle även alternativ D fungera. R5 låg på ett liknande sätt också lite mitt emellan de båda alternativen. Anledningen till velandet för R5 var främst att personen ansåg att man borde diskutera frågan med några involverade. Då alternativ D var att man inte diskuterade med någon och alternativ E var att man diskuterade med alla blev det därför en svår avvägning. Personen påpekade också att det oftast inte är utvecklarens roll att göra de kritiska säkerhetstesterna men att man som utvecklare i alla fall kan påpeka bristerna.

Tabell 8: Valt svarsalternativ på scenario 1

Respondent	**Val av åtgärd**	**Eventuell kommentar om valet**
R1	Slutför arbetet med alla funktionella krav först för att efteråt testa om det finns en möjlighet för integritetsintrång (C).	
R2	Utvecklar och implementerar en integritetsskyddande strategi tillsammans med alla involverade (E).	
R3	Utvecklar och implementerar en integritetsskyddande strategi tillsammans med alla involverade (E).	
R4	Utvecklar och implementerar en integritetsskyddande strategi tillsammans med alla involverade (E).	I brist på tid skulle personen valt alternativ D.
R5	Utvecklar och implementerar själv en integritetsskyddande strategi (D).	Vill egentligen inte utveckla strategin själv, men anser inte heller att det är nödvändigt att involvera alla.

4.4.2 Scenario 2

Följande scenario är direkt taget och översatt från Bu et al. (2020):

"Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. Företaget ber Tom skapa ett kryphål i programmet där de kan samla in affärsinformation i syfte att användas för interna analyser. Företaget planerar inte att informera användaren om denna åtgärd. Om du var Tom, vad hade du valt att göra? Välj det alternativ som passar in bäst med din åsikt.

A. Det är mitt företags beslut. Jag kommer följa instruktionerna och slutföra mitt arbete enligt de krav jag fått.
B. Jag anser att företagets förfrågan kränker användarens integritetsrättigheter och därför kommer jag ta upp detta med projektgruppen och hoppas på att företaget kan diskutera detta med vår kund först. Jag kommer bara slutföra mitt arbete enligt företagets krav om jag får användarens tillåtelse.
C. Jag tycker att företagets krav är förståeliga samtidigt som våra kunder har rätt att bli informerade. Därför kommer jag utföra företagets önskemål samtidigt som jag berättar för kunden om kryphålet.
D. Jag tycker att företagets önskemål bryter mot integritetsrättigheter. Trots detta kommer jag slutföra mitt arbete enligt företagets önskemål med oron för hur företaget annars kommer tänka kring mitt agerande.
E. All insamlad information kommer endast att användas för företagets interna analys och kommer därmed inte tillgängliggöras för andra. Därför tycker jag att företagets beslut är förståeligt och kommer slutföra mitt arbete."

Det andra scenariot är alltså mer inriktat på etik och moral kopplat till integritet. Frågan går ut på att intervjupersonerna får ta ställning till hur de hade agerat om deras arbetsgivare bett dem skapa ett kryphål i ett program till en kund för att samla in affärsinformation. Detta ska bara användas för interna analyser men arbetsgivaren önskar att det sker utan kundens vetskap. På denna frågan var alla intervjupersoner i stort sett helt överens om att alternativ B var det bästa valet. Alternativ B var att man ansåg att arbetsgivarens önskemål kränker kundens integritetsrättigheter och att man kommer ta upp detta med projektgruppen. Man kommer därefter endast utföra sitt arbete om kunden får reda på och godkänner kryphålet.

R1 velade mellan alternativ B och C, där alternativ C innebar att man själv berättade för kunden om kryphålet och sedan fortsatte sitt arbete. Till slut bestämde sig personen för att B var det man borde göra, men att C kanske är mer likt så som personen brukar gå till väga. Anledningen att R1 ansåg att det var viktigt att underrätta kunden om kryphålet var för att personen själv ville kunna känna sig stolt över det byggda systemet. R2 valde alternativ B utan några direkta tveksamheter. Motiveringen till detta var att personen av principskäl inte ville göra något sådant men samtidigt ville vara lojal mot sin arbetsgivare och därför ta upp diskussionen med dem först. Personen nämnde också att beroende på diskussionens utfall skulle denne fundera över om denne verkligen ville jobba där.

R3 ansåg i sin tur att svaret berodde på vilken situation man var i, alltså om man var konsult eller anställd. Personen poängterade att är man konsult har man ofta stöd hos sin konsultchef och kan rådfråga denna om det sker meningsskiljaktigheter på arbetsplatsen. Till slut bestämde sig personen för alternativ B eftersom denne tyckte det var något orätt som bör diskuteras men som man inte bör involvera kunden i om det inte är absolut nödvändigt. R4 valde, precis som de föregående intervjupersonerna, alternativ B. R4 var dock den enda som

uttryckte en viss oro över att bli avskedad om man stack ut hakan och ställde arbetsgivaren mot väggen. Svaret blev därmed *"Jag skulle ju vilja agera som på B, om jag har ekonomisk möjlighet att ta ett annat jobb."*.

R5 var precis som R1 till en början inne på svarsalternativ C. R5 menade dock att man inte behövde göra någon särskilt stor grej av det utan att det i princip kunde räcka att sätta upp en lapp till kunden om att man samlar in viss affärsinformation. Personen var sedan av den åsikt att om kunden inte reagerade på detta eller tog upp det hade man deras godkännande. Efter ett tag pekade R5 ut både alternativ B och C som relevanta men lutade till slut fortfarande mer mot alternativ C. Detta för att personen inte ansåg att det behövdes någon diskussion mellan kunden och arbetsgivaren utan att det borde räcka med den informerande lapp som det talades om tidigare.

Tabell 9: Valt svarsalternativ på scenario 2

Respondent	**Val av åtgärd**	**Eventuell kommentar om valet**
R1	Berättar själv för kunden om kryphålet och fortsätter sedan arbetet (C).	Personen ser egentligen B som det rätta svaret, men har oftast själv gjort alternativ C.
R2	Önskemålet kränker kundens integritetsrättigheter och detta kommer tas upp med projektgruppen. Slutför arbete vid godkännande från kunden (B).	
R3	Önskemålet kränker kundens integritetsrättigheter och detta kommer tas upp med projektgruppen. Slutför arbete vid godkännande från kunden (B).	
R4	Önskemålet kränker kundens integritetsrättigheter och detta kommer tas upp med projektgruppen. Slutför arbete vid godkännande från kunden (B).	
R5	Berättar själv för kunden om kryphålet och fortsätter sedan arbetet (C).	

5 Diskussion

5.1 Systemutvecklares syn på integritet

I litteraturgenomgången togs det upp hur systemutvecklares syn på integritet har en betydelsefull roll för systemutvecklingen samt att man många gånger upplever osäkerhet under diskussioner kring ämnet. Svaren kring den professionella synen på integritet var varierande. Ett samband vi tycks finna är däremot att systemutvecklarna med större integritetsansvar ofta tyckte det var viktigare med integritet även när de agerade som användare till skillnad från de som inte hade något större ansvar över integritetshanteringen i systemutvecklingsprocessen. De andra var mer eller mindre medvetna om riskerna men hade en ganska obrydd inställning till ämnet. Detta skulle kunna bero på att de inte ser de direkta riskerna lika tydligt eller ur samma synvinkel som de systemutvecklare som planerar och arbetar med hanteringen av integritet inom systemen. De intervjupersoner som arbetat med känslig data visade alltså på ett större ansvarstänk.

Precis som Hadar et al. (2018) påstod var det ingen av intervjupersonerna som var riktigt säkra på hur man skulle hantera implementeringen av integritet på ett korrekt sätt och de upplevde även begreppet som något otydligt i sin yrkesroll. Riktlinjer finns det gott om, men gällande hur dessa ska implementeras finns det stora tveksamheter och oklarheter kring. Enligt Hadar et al. (2018) ses även integritet som ett teoretiskt, abstrakt och opraktiskt koncept för många systemutvecklare. Även vi kunde se detta mönster hos intervjupersonerna. R4 och R5 tog framför allt upp diskussionen kring att integritetshanteringen ibland kunde vara väldigt opraktisk. Man ser helt enkelt hellre att användarna får acceptera en viss datainsamling för att ta del av vissa tjänster än att slå knut på sig själva för att lösa optimal integritetshantering. R5 menade att man ibland får bita i det sura äpplet som användare gällande datainsamling. Personen menade att man måste kunna hålla det enkelt och då kan det hända att integriteten får lida ibland.

I studien av Hadar et al. (2018) togs det också upp att integritetsbeslut tenderar att bero mer på sociala normer än lagar och tekniska riktlinjer, vilket är en trend vi inte har märkt av i våra intervjuer. För våra intervjupersoner skulle vi nästan vilja hävda motsatsen. Intervjupersonerna verkade inte influeras särskilt av sin sociala omgivning. Besluten verkade snarare tas efter den lösning som påverkade funktionaliteten så lite som möjligt och samtidigt levde upp till rådande lagstiftning, alltså GDPR. Integritet prioriterades i den mån att man skulle efterleva GDPR, men inte mycket mer än så. Vi ställer oss därmed tveksamma till att annorlunda sociala normer hade ändrat systemutvecklarnas beteende.

Något som genomgående stack ut en del under intervjuerna gällande systemutvecklarnas egen syn på integritet var R5s svar. Personen uttryckte sig ofta på ett ganska obesvärat sätt kring integritet och talade även om Organisationen i termer som obrydd när vi frågade om integritetshanteringen. Även om detta tyder på vissa skillnader i synsätt tar vi även i beaktning att detta utstickande sätt att formulera sig på kan bero på andra faktorer. Till exempel skulle

det likväl kunna bero på att R5 kände sig mer avslappnad och ärlig i hur denne uttryckte sig än de övriga intervjupersonerna.

5.2 Privacy by Design

Intervjupersonerna hade i de flesta fall hört talas om begreppet Privacy by Design, men inte mycket mer än så. Det var inget välkänt för dem och därmed inte heller något de använde i sitt arbete. Privacy by Design liknar och återfinns dock till stor del i andra dataskyddsregleringar som till exempel GDPR. Därför kommer vi att i fortsättningen koppla de utmaningar med Privacy by Design som nämns i litteraturgenomgången till utmaningar med generell integritetshantering. Detta för att vi anser att dessa stämmer överens i så pass hög grad att man kan göra en sådan koppling. Under intervjuerna gjorde vi också en intressant reflektion gällande just begreppet integritet. När vi ställde frågor om ämnet benämnde vi frågeställare det som just integritet medan varje gång intervjupersonerna svarade på dessa frågor omnämndes nästan enbart GDPR.

Integritet verkade således vara direkt kopplat till GDPR för systemutvecklarna. Självklart är GDPR riktlinjer för hur man ska hantera personlig data och därmed bevara integritet. Vi hävdar dock att begreppet integritet sträcker sig längre än GDPR. Integritet innefattar också sådant som de principer och ramverk vi presenterat men som förbisetts då efterlevnaden av GDPR setts som tillräcklig. Det går nästan alltid att skapa bättre integritetsskydd genom diverse åtgärder så som Privacy by Design och Privacy Impact Assessment. Alla dessa krävs inte för att uppnå GDPR, men ingår enligt oss i begreppet integritet och därför menar vi att integritet inte är begränsat enbart till GDPR. Anledningen till att systemutvecklare ser integritet som synonymt med GDPR kan tänkas bero på att de är vana vid att förhålla sig till just GDPR. Det är de riktlinjer man måste förhålla sig till enligt lagen och det är den mest omtalade lagstiftningen inom ämnet.

Integritetstänket verkade alltså inte vara större än det som framtvingats av rådande lagstiftning. Den europeiska lagstiftningen som finns är dock ganska långtgående och erbjuder ett bra integritetsskydd. Därmed är det inget problem att enbart följa lagstiftningen. Frågan man kan ställa sig är snarare hur systemutvecklarnas inställning hade varit om lagstiftningen inte varit så omfattande. Alltså, är systemutvecklarna nöjda med den nivå av integritet vi har idag för att de faktiskt tycker att det är en rimlig nivå eller för att de inte bryr sig längre än att följa lagstiftningen? Det är svårt att ge svar på, speciellt då det inte är det som studien ämnade undersöka. Men vi anser att det är en intressant aspekt att ha i åtanke.

5.3 Utmaningar med integritetshantering

Det första påståendet kring att riktlinjerna och ramverket gällande integritet ofta är vaga (Martin, del Alamo & Yelmo, 2014) verkar stämma bra då det under intervjuerna uttrycktes en del oklarheter kring dessa. Intervjupersonerna nämnde bland annat att det är svårt att veta vad riktlinjerna egentligen innebär, att det finns för stor tolkningsfrihet och att de är svåra att omsätta i praktiken. Detta bekräftar således Martin, del Alamo & Yelmos (2014) andra påstående om att systemutvecklare ofta saknar detaljerade riktlinjer innehållandes tydliga instruktioner för implementering av de tekniska bitarna. Anledningen till detta tycks vara att

riktlinjerna utformas av jurister och därmed inte får den konkreta, tekniska aspekt som skulle behövas.

En intervjuperson efterfrågade just konkreta exempel på hur man skulle gå till väga. Detta tror vi dock blir svåruppnåeligt eftersom inget system är det andra likt. Ett konkret exempel fungerar därmed bara för ett liknande system som det i exemplet. Skiljer sig systemen åt är vi tillbaka på ruta ett där det finns alldeles för mycket tolkningsutrymme. Längre fram i tiden lär det som sagt komma prejudikat och då också konkreta exempel, men även dessa kommer inte alltid vara möjliga att gå efter då fallet är väldigt situationsberoende. Man kommer aldrig kunna gå ner på detaljnivå i några exempel för då gäller helt plötsligt exemplen bara för vissa system.

Vidare tog även Spiekermann (2012) upp att många tjänster lätt går förlorade vid begränsningen av insamlandet av data. Detta fick vi till viss del bekräftat när en av intervjupersonerna nämnde att de på Organisationen gått från att i snitt ha 12-13 cookies till att bara ha 1. Personen ansåg att begränsningen försvårat arbetet rejält, men skulle dock inte vilja ha det ogjort då personen också har stor förståelse för varför dessa begränsningar införts. Spiekermann (2012) ställde sig också i slutet av sin artikel frågan om det verkligen finns några egentliga fördelar med att investera i Privacy by Design för organisationer. Just den studerade organisationen verkar, liksom Spiekermann (2012), inte se någon vinst med detta då integritet bara fanns i form av att följa GDPR som en del av systemutvecklingsprocessen.

En intressant aspekt gällande avsaknaden av en specifik integritetsstrategi är att R5 motiverade detta med att Organisationen inte hanterade särskilt mycket persondata medan R2 ansåg att Organisationen hanterade väldigt mycket persondata. En sådan stor skillnad i synsättet är svår att förklara men antagligen beror det dels på olika värderingar av integritet som begrepp men också att R2 verkar ha arbetat med känslig data i större utsträckning. Något majoriteten dock påpekade var att Organisationen oftast inte bygger nya system utan att de uppdaterar och arbetar vidare på redan existerande system och att det därmed är svårt att bädda in integritet i processen. Men borde Organisationen införa en specifik integritetsstrategi då? Vi ser faktiskt inget större behov av detta då Organisationen är en verksamhet inom den offentliga sektorn och inget kommersiellt företag. Anledningen till att kommersiella företag är i större behov av en integritetsstrategi menar vi är för att den insamlade datan ses mer som en tillgång där. Precis som Spikermann (2012) tog upp så är personlig data hos kommersiella företag ofta en stor tillgång och utan den är det lätt att värdefulla tjänster hos företaget går förlorade. Denna risk finns inte hos verksamheter inom den offentliga sektorn. Dessutom blir det svårt för Organisationen att fastställa en strategi som är användbar i alla projekt då projektets omfång till stor del beror på hur stora ändringar som ska göras.

Enligt Schwartz (2009) lägger företag idag mer energi på att utbilda sina anställda inom Privacy by Design, eller integritetshantering, för att skapa större ansvarstagande. Hadar et al. (2018) fann i sin studie att det sker en del ansvarsförskjutning gällande integritet. Vi har svårt att varken bekräfta eller dementera detta då både R3 och R5 påpekade att de inte såg integritet som en del av sitt arbete men samtidigt valde svarsalternativ som reflekterade ett högt ansvarstagande i scenarioanalysen. Den ökade satsningen på utbildning kunde vi dock se i våra intervjuer då intervjupersonerna ofta nämnde utbildningar de haft inom området. Dock verkar inte utbildningarna föra med sig så pass mycket som man kanske hade hoppats på. De ökar såklart medvetenheten om integritetsfrågor men verkar inte göra mycket mer än så. Eftersom riktlinjerna, som vi tidigare nämnde, är allt för svåra att efterfölja och inte ens de som håller i utbildningarna kan ge några riktiga svar på hur man borde gå till väga blir vår tolkning att de inte är särskilt givande. De flesta var också överens om att de på

Organisationen arbetar aktivt med att hålla sig uppdaterade kring nya teknologier, vilket i sig också är en typ av utbildning. Det främjar medvetenheten inom området och ser till att systemutvecklarna alltid sitter med den senaste kunskapen när problem uppstår vilket skapar moderna, och därmed mer säkra, lösningar.

5.4 Integritet i systemutvecklingsprocessen

Hadar et al. (2018) delade in hanteringen av integritet hos system i två delar, *privacy-by-architecture* och *privacy-by-policy.* De genomförda intervjuerna visade på att *privacy-by-policy* var den del som det lades mest fokus på inom Organisationen och konceptet med *privacy-by-architecture* togs inte upp av deltagarna. Därav tolkar vi det som att användandet av den typ av integritetshantering är väldigt begränsad. R3 berättade även att systemen de arbetar med ofta var undersökta och genomtänkta innan de skickades vidare till personen. Detta skulle kunna förklara varför användningen av *privacy-by-architecture* verkade vara begränsad då det måste implementeras tidigt i systemutvecklingsprocessen.

Som tidigare nämnt fick vi under intervjuerna ett intryck av att integritetstänket mestadels gick ut på att leva upp till de begränsningar som kommer med GDPR. Utöver det fanns det inga klara strategier eller principer som man försökte efterleva inom organisationen vilket kan vara en av anledningarna till att systemutvecklarna främst kopplar integritet till GDPR. Teorin från Bu et al. (2020) kring hur det omgivande klimatet spelar roll för hur systemutvecklare värderar integritet kan vi varken bekräfta eller dementera. Då det inte riktigt fanns något direkt organisatoriskt klimat gällande integritet på Organisationen är det svårt att ta ställning till detta. Vi såg dock att systemutvecklares egna erfarenheter och preferenser gällande integritet till stor del speglade de beslut de tog, vilket Bu et al. (2020) också fann i sin studie.

De områden som aktivt lyfts upp av organisationen brukar automatiskt också uppmärksammas mer bland utvecklarna. Organisationen verkar i detta fall ha valt att enbart lägga kraft och fokusera på integritet genom implementeringen av GDPR vilket gjort att eventuella ytterligare integritetsskyddande lösningar prioriteras bort. Det bör noteras att eftersom Organisationen inte använder persondata i kommersiellt syfte och bara samlar in precis den data som behövs kan det vara svårt att hitta ytterligare lösningar för att skydda integriteten. Dock är det svårt att hitta något man inte heller letar efter. Även om Organisationen i många fall inte hade kunnat öka integritetsskyddet så mycket mer än till just den nivån som krävs enligt lagen tror vi att det i vissa fall absolut hade kunnat göras förbättringar om drivkraften funnits där.

Enligt Bu et al. (2020) kan man ofta se en reflektion av systemutvecklarens beteende och tankesätt i produkterna de utvecklar då det oftast är de som har det största ansvaret för slutprodukterna. Slutprodukten från en systemutvecklare som tar stor hänsyn till integritet kommer alltså skilja sig en del från slutprodukten från någon som inte tar samma ansvar. Det här mönstret kunde vi också på sätt och vis se i vår studie. De systemutvecklare som svarade att de som användare var bekymrade över bristen på integritet på nätet var även de som verkade extra måna om integritetshanteringen i sina yrkesroller. Vi kan dessvärre inte dra någon slutsats om just skillnader i de olika personernas slutprodukt beroende på inställningen till integritet då vi inte undersökt detta. Något som vi däremot kan bekräfta är att personerna med mer respekt för integritet också hade en större medvetenhet kring detta under systemutvecklingsprocessen.

Om vi då går tillbaka till de två olika sätten att tackla integritetshantering, *privacy-by-architecture* och *privacy-by-policy*, skulle man kunna diskutera att man genom implementering av *privacy-by-architecture* kanske kan eliminera risken för att systemutvecklares preferenser kring integritet genomsyrar det färdiga systemet. Genom att kombinera dessa två delar skulle man indirekt bli tvingad till att följa fler riktlinjer och policies än vad lagen kräver. Detta skulle i sin tur kunna resultera i att systemutvecklares preferenser inte märks av lika tydligt i systemen vilket är en positiv utveckling om systemutvecklarens attityd gentemot integritetshantering är för avslappnad. Att kombinera *privacy-by-architecture* och *privacy-by-policy* är att rekommendera framför allt för att den förstnämnda kan förhindra att användarens integritet kränks enbart genom bra arkitektur (Hadar et al., 2018). En sådan här lösning skulle kunna minska risken för att systemutvecklares preferenser bidrar till en bristfällig integritetshantering.

I studien som Bu et al. (2020) utförde kunde man se att implementeringen av Privacy by Design var något som ansågs öka arbetsbelastningen. Då de flesta av intervjupersonerna inte hade någon större bekantskap med principerna från begreppet Privacy by Design kan vi vare sig förneka eller bekräfta detta. Däremot kunde vi se att de som arbetade med integritet ansåg att arbetsbelastningen ökade samt att de som inte arbetade med integritet var lättade över detta. Därmed kan vi dra slutsatsen att även om vi inte har tillräckligt med empiri för att bedöma arbetsbelastingen av just Privacy By Design så finns det ett stöd i vår studie för en känsla av ökad arbetsbelastning i samband med integritetshantering. Värt att nämna är att Bu et al. (2020) utfört sin studie i Kina där regeringens syn på integritet skiljer sig från den allmänna syn som finns i Europa. Även om studien utförts på personer inom IT-sektorn och inte på människor som är aktiva inom regeringen är det viktigt att ha i åtanke att klimatet i landet skiljer sig från klimatet i Sverige och skulle kunna påverka de anställdas syn på ämnet.

Bu et al. (2020) kunde också se en tydlig koppling mellan incitament, systemutvecklarnas syn på Privacy by Design samt användningen av principerna. Precis som vi nämnde ovan var denna slutsats svår att dra för oss då deltagarnas bekantskap med principerna var begränsad. Några tydliga incitament tycks vi inte finna varken gällande implementeringen av Privacy by Design eller implementeringen av GDPR som var mer aktuellt för våra intervjupersoner. Detta skulle kunna bero på att Organisationen i dagsläget endast genomför de åtgärder som krävs av lagstiftningar.

Organisationen har ingen policy varken för hur potentiella risker ska identifieras eller för hur integritet ska hanteras i systemutvecklingsprocessen. Detta motiverades med att Organisationen sällan byggde system utan oftast utvecklade redan existerande system. Vi anser dock att Organisationen hade gynnats av att använda sig av exempelvis Privacy Impact Assessment-metodiken som Ahmadian et al. (2018) skapade då denna kan utföras på redan existerande system. Även om Organisationen bara uppdaterar ett system kan man gynnas av att ha integritet i åtanke när man skapar de nya lösningarna för systemet. Alla uppdateringar och ändringar är självklart annorlunda och har olika omfång, men genom att ha ett systematiskt sätt att hantera detta på menar vi att man får ännu ett kvalitetssäkrande steg i processen.

5.5 Scenarioanalys

Scenarierna är direkt tagna och översatta från studien av Bu et al. (2020). Bu et al. (2020) förklarar inte vid presentationen av scenarierna hur svaren bör tolkas eller hur de själva gått

till väga för att tolka svaren. Vi gör därmed en fri tolkning relaterad till våra forskningsfrågor utifrån de svar vi fått. Det första scenariot gav en större spridning i svaret än vad den andra gjorde. Detta visar på hur samma typ av utvecklare på samma Organisation fortfarande kan skilja sig åt i sitt tankesätt. Studien från Ayalon et al. (2017) som visade att det organisatoriska klimatet påverkade integritetsbesluten mer än den rättsliga bakgrunden kan därmed ifrågasättas i just det här fallet. Trots att intervjupersonerna arbetade i samma miljö skiljde sig besluten åt. Dock kan vi konfirmera att deras personliga upplevelse av integritet påverkar designbesluten som studien av Ayalon et al. (2017) också visade. Personer som var mer bekymrade över integritet i privatlivet verkade också ha ägnat det mer åtanke även i sin yrkesroll.

Den första frågan gällde som tidigare nämnt ansvarstagande kring integritet. Alla intervjupersoner valde ett alternativ som innebar någon form av ansvarstagande. R1 valde ett mindre ansvarstagande alternativ och sa själv att personen inte hade gett integritetshanteringen hög prioritet. R1 är också den person som arbetar som frontend-utvecklare medan resterande arbetar som fullstack-utvecklare. Detta tror vi kan ha påverkat R1 då personen antagligen inte är med i lika stor utsträckning av systemets livscykel och därmed inte ser sig ha riktigt samma nivå av ansvar. Dessutom nämnde personen själv under intervjun att denne hade svårt att se integritet som en del i just frontend-utveckling, vilket också troligen varit en bidragande faktor till svaret. Även om alla svarade att de hade tagit ansvar över integritetsarbetet var det med väldigt olik prioriteringsgrad och omfattning.

Den andra frågan behandlade etiska och moraliska aspekter gällande integritet. Det vi kunde se var att svaren nästan var helt eniga gällande den andra frågan. Detta skulle kunna förklaras av att människor i större utsträckning har samma etiska och moraliska principer, alltså att de flesta är överens om vad som är rätt och vad som är fel i en situation. Vad man ser som sitt eget ansvar, eller sin egen arbetsuppgift, verkar alltså variera i större skala än vad man anser vara moraliskt rätt. Även om svaren skiljde sig åt en aning mer på den första frågan valde intervjupersonerna generellt ganska lika svarsalternativ. Besluten de tar i sitt arbete torde därmed också vara rätt lika, men en intressant aspekt var att trots de liknande svaren hade intervjupersonerna relativt olika anledningar till sitt val. Dessutom kommenterade vissa att de hade velat göra något som inte fanns som ett alternativ. Till exempel valde R4 mellan alternativ D och E på den första frågan då personen menade att svaret berodde på hur mycket tid man hade på sig. På så vis vägde personen in en aspekt som inte nämndes i frågan och som inte heller påtalades av någon annan intervjuperson. R5 låg också mellan alternativ D och E på den första frågan, men av en helt annan anledning. För R5 var problemet i stället att personen hade velat göra något mellanting mellan alternativen.

Även på den andra frågan uppstod den här typen av olikheter. De allra flesta valde alternativ B baserat på att de tyckte förfrågan kändes moraliskt fel och inte ville stå för något sådant. R5 valde alternativ C som låg väldigt nära B och också var ett moraliskt bra alternativ. Motiveringen till detta var dock snarare att avsäga sig ansvaret än att uppgiften var moraliskt fel att utföra. Att det slutgiltiga beslutet kan vara samma men att vägen dit, och anledningen till beslutet, kan skilja sig åt så mycket är ett intressant fynd som vi inte hade väntat oss att få ut av studien. Upptäckten är dock ganska värdefull då den pekar mot att systemutvecklares attityd till integritet till stor del avgör hur de tar sina beslut, även om besluten i slutändan blir desamma.

6 Slutsats

Syftet med den utförda studien var att undersöka ifall systemutvecklares attityd gentemot integritet påverkar deras beslut i systemutvecklingsprocessen. Detta har vi gjort genom att försöka besvara följande forskningsfrågor:

Hur aktivt är integritetstänket bland enskilda systemutvecklare i systemutvecklingsprocessen?

På vilket sätt genomsyrar de enskilda systemutvecklarnas egna erfarenheter och preferenser integritetstänket?

Resultatet av vår studie pekar på att det inte finns ett aktivt integritetstänk större än det som framtvingats av rådande lagstiftning, men det är svårt att avgöra om detta beror på att lagstiftningen har en bra integritetsnivå eller om det saknas intresse för att göra mer än vad lagen kräver. Intresset för att hålla sig uppdaterade med ny teknologi samt att uppnå den lagstiftning som finns gällande integritet är stort, men att göra fler åtgärder än så anses överflödigt. Att systemutvecklare, och organisationer i sig, har detta förhållningssätt till integritet är föga förvånande. Att lägga ytterligare krafter på integritet är kostsamt och tidskrävande och anses därför ofta inte ge tillräckligt många påtagliga fördelar. Man skulle även kunna vänta sig att ökad integritetshantering skapar en ökad arbetsbelastning som ses negativt på av systemutvecklarna, men till vår förvåning såg intervjupersonerna inte det som ett större problem. Alla intervjupersoner var överens om att funktionaliteten ibland behöver kompromissas på grund av integritetskrav men hade förståelse för att detta merarbete behövs för att följa lagstiftningen. Gällande hur systemutvecklarnas egna erfarenheter genomsyrar integritetstänket i systemutvecklingsprocessen kan vi konstatera att hur systemutvecklare tar beslut gällande integritetsfrågor och vad de grundar dessa på till stor del beror på den egna synen på integritet.

En intressant och lite oväntad observation som gjordes var även att samtliga deltagare i studien främst förknippade integritet med GDPR. När integritetshantering diskuterades var det enbart GDPR som kom på tal trots att det finns andra principer att tillämpa. Detta skulle kunna förklaras med att brott mot lagen har större konsekvenser än bristande användning av principer och att de därför lätt glöms bort. Då integritet nästan enbart talades om i form av GDPR under intervjuerna kan vi därmed dra slutsatsen att GDPR, och inte bara integritetshanteringen generellt, saknar tydliga direktiv och konkreta exempel. Även om GDPR lägger en bra grund för integritetshanteringen kan det vara svårt för organisationer att omsätta detta i praktiken. Det finns således fortfarande mycket kvar att göra inom området för att underlätta skapandet av ett bra integritetsskydd.

Något annat som också överraskade oss var att trots att intervjupersonerna hade liknande bakgrund, flertalet utbildningar inom ämnet och höll sig kontinuerligt uppdaterade gällande de senaste teknologierna skiljde sig tankesätten och synen på integritet så pass mycket. Utbildning kan således fungera i den mån att informera systemutvecklarna om hur man borde gå till väga och varför, men verkar inte kunna skapa en enhetlig syn på, och prioritering av,

integritet. Genom denna studie önskar vi kunna bidra till ökad kunskap inom akademin då studierna inom ämnet är något begränsade i dagsläget. För organisationer och yrkesutövare hoppas vi med dessa fynd bidra till ökad förståelse för systemutvecklares attityd till integritetshantering och öppna upp för fler diskussioner bland de involverade parterna.

6.1 Förslag till vidare forskning

Den här studien är en del av ett relativt outforskat område som vi menar förtjänar mer uppmärksamhet. Vi vill därför uppmuntra andra akademiker och forskare inom digital integritet att antingen replikera denna studie eller att göra en annan studie på samma område. Att replikera vår studie hade varit gynnsamt för att kunna verifiera de resultat och den slutsats vår studie resulterade i. Att göra en ny studie hade till exempel skapat en möjlighet att istället studera systemutvecklare på ett kommersiellt företag som behandlar mer känslig data och har större ekonomisk vinning i att undvika att skydda användarnas integritet. Det skulle även vara intressant att göra en jämförelse mellan systemutvecklare på exempelvis verksamheter inom den offentliga och privata sektorn i hur de ser på och hanterar integritet i systemutvecklingsprocessen.

Bilaga 1 - Intervjuguide

Introduktion:

1) Välkomna och tacka för att de ställt upp på intervju.

2) Presentera oss och studiens syfte, varför vi är här idag.

3) Berätta om insamlandet av kunskap inför intervjun.

4) Fråga om tillåtelse att spela in intervjun.

Uppvärmningsfrågor:

1) Vad är din roll i verksamheten? Vad innebär det?

2) Hur ser en typisk arbetsdag ut?

Förhållande till integritet:

1) Hur ser du på personlig integritet i allmänhet?

2a) Vad betyder begreppet digital integritet/privacy för dig?

2b) Ser du på det på olika sätt som användare/utvecklare?

3a) Finns det i ditt arbete? Ja/nej? Utveckla.

3b) Om ja, hur arbetar du i så fall med integritet?

3c) Skulle du vilja arbeta annorlunda med integritet?

Strategi kopplad till integritet:

1a) Känner du till begreppet Privacy by Design?

1b) Om ja, är det något du använder i, eller kan relatera till, ditt arbete?

2) Vill du beskriva ett projekt som har behandlat personuppgifter på något sätt lite mer ingående, i den mån du kan?

3) Händer det i utvecklingsprocessen att ni ifrågasätter om ni verkligen behöver vissa uppgifter?

4) Har ni några policies eller normer för hur man arbetar med digital integritet i era projekt?

5) Har ni några etablerade metoder för att identifiera olika risker eller designval som skulle kunna förbättras gällande hanteringen av integritet (privacy)?

6a) Arbetar ni aktivt för att hålla er uppdaterade med den senaste teknologin gällande integritet?

6b) Om så är fallet, hur?

Scenarier:

Följande scenarier är direkt tagna och översatta från Bu, F., Wang, N., Jiang, B. & Liang, H. (2020). "Privacy by Design" implementation: Information system engineers' perspective, *International Journal of Information Management,* vol. 53:

1) "Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. I projektet finns det en väldigt tydlig arbetsfördelning gällande inloggningsautentisering, verifiering vid betalning, affärsfunktioner etc. Tom är ansvarig för utvecklingen av några affärsfunktioner gällande användare, skapandet av ett användargränssnitt samt kopplingen mellan front- och back-end. Om du var Tom, vilket av de följande alternativen stämmer bäst överens med din åsikt?

A. Mitt arbete involverar inte extern dataöverföring. Integritets- och säkerhetsrelaterade problem är inte en del av min uppgift, ansvaret borde ligga på de som testar säkerheten.
B. Att prestera på arbetet är viktigt för mig och jag borde slutföra mitt arbete så snart som möjligt. Integritets- och säkerhetsskydd är inte en kritisk fråga som jag behöver beakta.
C. Jag kommer slutföra mitt arbete så snart som möjligt. Jag kommer testa huruvida det finns en risk för integritetsintrång efter att alla funktionella krav är uppnådda.
D. Jag kommer beakta huruvida det finns risk för en integritetsläcka kopplat till det jag arbetar med och skapa en integritetsskyddande strategi. Sedan kommer jag slutföra mitt jobb så fort som möjligt.
E. Jag kommer diskutera den integritetsskyddande strategin med alla involverade för att sedan fortsätta med utvecklingen och implementeringen av den framlagda strategin."

Vad fick dig att välja det? Hur tänkte du?

2) "Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. Företaget ber Tom skapa ett kryphål i programmet där de kan samla in affärsinformation i syfte att användas för interna analyser. Företaget planerar inte att informera användaren om denna åtgärd. Om du var Tom, vad hade du valt att göra? Välj det alternativ som passar in bäst med din åsikt.

A. Det är mitt företags beslut. Jag kommer följa instruktionerna och slutföra mitt arbete enligt de krav jag fått.
B. Jag anser att företagets förfrågan kränker användarens integritetsrättigheter och därför kommer jag ta upp detta med projektgruppen och hoppas på att företaget kan diskutera detta med vår kund först. Jag kommer bara slutföra mitt arbete enligt företagets krav om jag får användarens tillåtelse.
C. Jag tycker att företagets krav är förståeliga samtidigt som våra kunder har rätt att bli informerade. Därför kommer jag utföra företagets önskemål samtidigt som jag berättar för kunden om kryphålet.
D. Jag tycker att företagets önskemål bryter mot integritetsrättigheter. Trots detta kommer jag slutföra mitt arbete enligt företagets önskemål med oron för hur företaget annars kommer tänka kring mitt agerande.
E. All insamlad information kommer endast att användas för företagets interna analys och kommer därmed inte tillgängliggöras för andra. Därför tycker jag att företagets beslut är förståeligt och kommer slutföra mitt arbete."

Vad fick dig att välja det? Hur tänkte du?

Bilaga 2 – Transkribering intervju 1

I följande bilaga kommer det som tidigare benämnts scenario refereras till som casefrågor.

FS1: Sådär ja, ja men då skulle vi vilja börja med att fråga vad är det du arbetar med? Vad är din roll i verksamheten?

R1: Jag är, nu ska vi se här… Frontend-utvecklare och accessibility-ansvarig för den externa webben för Organisationen.

FS1: Okej, och vad innebär det?

R1: Jag är ansvarig för all frontend till alla drupal CMS-sidor vi använder. Så 260 siter eller något sådant.

FS2: Oj, det är mycket arbete.

R1: Nja, det är samma cloud-bas så det är rätt lugnt.

FS2: Hur ser en arbetsdag ut? Skulle du kunna beskriva?

R1: Ehmm.. Vi kör några timmars utveckling, sen kör vi daily scrum, sen kör vi utveckling, massa möten, mer utveckling. Framförallt nu i corona så är det väldigt mycket utveckling och väldigt lite annat.

FS1: Jag förstår. Men vad var det där andra du sa? Du sa det var frontend och…?

R1: Accesibility, usability framförallt.

FS1: Okej.

R1: Men det var för att min grundutbildning är inom informatik och usability. Så jag hjälper till med både att utveckla accessibility för avdelningen, se till så att den är mer anpassad för funktionsnedsatta samt hjälper till att utveckla accessibility och usability för externa webben på Organisationen. Göra den mer lättanvänd, lättnavigerad och funktionsnedsattsanpassad.

FS1: Okej. Vad var det för utbildning du hade gått?

R1: Jag gick web multimedia på Karlstad universitet som var en 50/50 systemvetenskap/informatik.

FS1: Hur ser du på personlig integritet i allmänhet?

R1: Det är en fruktansvärt bred fråga. Jag känner att ni får specificera den lite mer än så. Vilka aspekter av personlig integritet menar ni?

FS1: Vi tänker ju personlig integritet på nätet. Alltså i den frontend du utvecklar och designar till exempel hur ser du….

R1: Alltså jag har ju svårt att hitta personlig integritet i frontend utveckling över huvud taget. Jag har svårt att ens se den kopplingen. Det är därför jag behöver lite mer feedback om vad ni menar med frågan.

FS1: Ja, alltså, det är väl egentligen hur du som… Om vi tar det såhär då, som användare. Hur ser...

R1: Tänker ni typ GDPR-integritet där eller hur tänker ni?

FS2: Ja, alltså datahantering.

R1: Ja, okej! Det är enough. Det är väldigt svårnavigerat när det gäller frontenden för att så som de flesta i min generation utvecklade när vi var yngre så var det sessions och cookies som gjorde 80% av allt arbetet. Ehm, och att de inte går att använda på samma sätt längre gör det jävligt svårt att utveckla. Just att man inte kan spåra användarna inom sina egna system gör det jävligt svårt att utveckla effektivt och produktivt. Så vi har försökt hitta andra lösningar för att klara av de problemen men det är fortfarande svårt. När vi fick igenom GDPR-lagarna för staten så gick vi, jag tror vi gick från 12-13 cookies i snitt per användare till 1 som hade typ 5 minuters livstid. Så det gjorde så att all cachning och all inloggningsinformation blev fruktansvärt mycket mer svårhanterad.

FS1: Ja, precis.

FS2: Du tog upp att ni fick komma med andra lösningar och så. Kan du berätta lite om hur ni löste det?

R1: Alltså jag ska inte säga att vi löste det, vi fick komma på lösningar som kringgick det. Mer eller mindre så var det att vi fick designa om delar som använde cookies till att inte längre fungera så bra. Våra söksystem slutade acceptera cookies vilket gjorde så att vi tredubblade användningstiden och uppladdningstiden och gå över till system som push states framförallt inom JS, eller JavaScript, för att kunna enklare låta deras egna browser hålla koll på vad de behövde komma ihåg. Vilket var klyddigt och krävde jävligt mycket utvecklingstid,

men det gick. Men i mångt och mycket så i dagsläget har vi en cookie som säger "är du okej med cookies?", det är den enda cookien vi kan använda.

FS2: Skulle du säga att detta då bidragit till att funktionaliteten fått kompromissas?

R1: Ja, kraftigt.

FS1: Är det något du skulle velat ha ändrat på om du skulle ha möjligheten till det?

R1: Det är en jävligt bra fråga. Det tror jag inte.

FS1: Nej, okej.

R1: Jag älskar ju lagarna som de är. Säg att de gör mitt jobb jävligt mycket drygare och tråkigare, fine, men det gör även mitt användande av internet som privatperson jävligt mycket roligare.

FS2: Ja, det var det vi också pratat lite om - att hur man då ställer sig till det som utvecklare och sen som användare.

R1: Ja alltså jag ser ju mig mer som en internetanvändare än en internetarbetare så i slutändan är det ju mer av net positive för mig än negative.

FS1: Men hur känner du nu då, för nu var det ändå några år sedan GDPR infördes, så börjar ni få någon struktur på hur ni arbetar?

R1: [skratt] Nej.

FS1: Nej? Det är nya utmaningar varje gång?

R1: Alltså poängen är att jag har fruktansvärt många vänner och bekanta inom systemutveckling också och alla är överens om en sak; ingen vet riktigt vad GDPR innebär. Vi vet bara att vi måste anpassa oss till det.

FS1: Och är det för att det är lite otydligt?

R1: För att det kom väldigt hårda krav på att vi skulle GDPR-anpassa alltihopa men vi fick aldrig tid att lära oss vad GDPR innebar. Så de tog in en extern expert som sa "ja det här är bra, det här är dåligt". Ja jo, då har vi gjort vad de har pekat och sagt är bra och dåligt men vi har inte lärt oss någonting.

FS1: Nej, okej… Yes, vi förstår. Ehm... Ja, då skulle vi vilja presentera några casefrågor för dig.

R1: Kör!

FS2: Yes, jag ska bara ta fram dem här så delar jag min skärm.

FS1: Ja, det är mycket text så vi tänkte att det är bra om du ser den själv också.

FS2: Kan ni se nu?

FS1: Inte än.

R1: Nu så.

FS1: Caset är då:

Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. I projektet finns det en väldigt tydlig arbetsfördelning gällande inloggningsautentisering, verifiering vid betalning, affärsfunktioner etc. Tom är ansvarig för…

FS2: Ehm… är detta? Jag tror detta blev fel…

R1: Du säger inte det som står på skärmen iallafall.

FS2: Nej.

FS1: Nej jag läser den första frågan.

FS2: Jag vet inte om jag bara…

FS1: Annars kan vi ju ta den också, det kvittar ju ordningen på dem.

FS2: Så, nu tror jag det är rätt.

FS1: Ja precis. Så Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. I projektet finns det en väldigt tydlig arbetsfördelning gällande inloggningsautentisering, verifiering vid betalning, affärsfunktioner etc. Tom är ansvarig för utvecklingen av några affärsfunktioner gällande användare, skapandet av ett användargränssnitt samt kopplingen mellan front- och backend. Om du var Tom, vilket av de följande alternativen stämmer bäst överens med din åsikt?

F. Mitt arbete involverar inte extern dataöverföring. Integritets- och säkerhetsrelaterade problem är inte en del av min uppgift, ansvaret borde ligga på de som testar säkerheten.
G. Att prestera på arbetet är viktigt för mig och jag borde slutföra mitt arbete så snart som möjligt. Integritets- och säkerhetsskydd är inte en kritisk fråga som jag behöver beakta.
H. Jag kommer slutföra mitt arbete så snart som möjligt. Jag kommer testa huruvida det finns en risk för integritetsintrång efter att alla funktionella krav är uppnådda.
I. Jag kommer beakta huruvida det finns risk för en integritetsläcka kopplat till det jag arbetar med och skapa en integritetsskyddande strategi. Sedan kommer jag slutföra mitt jobb så fort som möjligt.
J. Jag kommer diskutera den integritetsskyddande strategin med alla involverade för att sedan fortsätta med utvecklingen och implementeringen av den framlagda strategin.

R1: Eh, klar C.

FS1: Klar C. Vad fick dig att välja klar C?

R1: För att det är det sättet jag arbetar på. Du bygger det först sen så testar du ifall det har gått åt helvete eller inte. Alltså, jag kommer testa den men det är inte en av de fyra viktigaste sakerna jag kommer börja med. Det ligger långt ner.

FS2: Vilka skulle du säga är de viktigaste grejerna?

R1: Nu är jag som sagt frontend-utvecklare så funktionalitet är det viktiga. Allting ska funka som det ska, kopplingarna ska vara rätt, du ska ha en ordentlig, shit vad fan heter det, metod för hur du kopplar back-enden till frontenden och när allt är på plats och den är funktionell då kommer jag säga "okej, kommer det finnas ett problem med integritet här? Kommer vi skicka över några personuppgifter". Och visst, det finns ju en snabbtanke när projektet börjar också, som är "kommer detta vara relevant" men i värsta fall får man bygga om en del av funktionaliteten när man inser att integriteten är kompromissad.

FS2: Mm. Och då är det lättare att göra det i ett senare skede?

R1: Alltså, för mig, jag tycker ju att det funktionella är det svåra att få bra. Så jag börjar alltid med att bygga det.

FS2: Då tar vi nästa. Jag vet inte varför det inte går att byta slide när jag delar.

FS1: Nej, det är lite skumt.

FS2: Vi pausar lite här så ska jag byta slide.

FS1: Det är ingen fara.

FS2: Så. Då ska vi se här: Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. Företaget ber Tom skapa ett kryphål i programmet där de kan samla in affärsinformation i syfte att användas för interna analyser. Företaget planerar inte att informera användaren om denna åtgärd. Om du var Tom, vad hade du valt att göra? Välj det alternativ som passar in bäst med din åsikt.

K. Det är mitt företags beslut. Jag kommer följa instruktionerna och slutföra mitt arbete enligt de krav jag fått.
L. Jag anser att företagets förfrågan kränker användarens integritetsrättigheter och därför kommer jag ta upp detta med projektgruppen och hoppas på att företaget kan diskutera detta med vår kund först. Jag kommer bara slutföra mitt arbete enligt företagets krav om jag får användarens tillåtelse.
M. Jag tycker att företagets krav är förståeliga samtidigt som våra kunder har rätt att bli informerade. Därför kommer jag utföra företagets önskemål samtidigt som jag berättar för kunden om kryphålet.
N. Jag tycker att företagets önskemål bryter mot integritetsrättigheter. Trots detta kommer jag slutföra mitt arbete enligt företagets önskemål med oron för hur företaget annars kommer tänka kring mitt agerande.
O. All insamlad information kommer endast att användas för företagets interna analys och kommer därmed inte tillgängliggöras för andra. Därför tycker jag att företagets beslut är förståeligt och kommer slutföra mitt arbete.

R1: Ehm… Den är lite svårare, men jag skulle hoppas på B. Men C är också väldigt relevant. Men nej, mer B.

FS1: Mer B, varför det?

R1: Alltså jag tycker allt bör diskuteras med kunden men det är tyvärr en del av både B och C. Men jag tycker ju att insamlande av information… Alltså idealisten i mig vill ju berätta det

för användaren, men som sagt, det jag tycker man borde göra är B men det jag oftast gör är nog C.

FS1: Mm, precis. Är det för att du känner att du har vissa skyldigheter gentemot kunden eller…

R1: Mm.

FS1: Eller är det för att du kan relatera till…

R1: Nej, alltså egentligen jag skiter både i företaget och kunden, det viktiga för mig är att jag kan vara stolt över det jag har byggt. Och de få kryphålen jag själv programmerar in det är ju easter eggs för min egen skull. Jag skulle aldrig göra någonting som på något vis kan skada användaren.

FS1: Nej, exakt. Yes, men toppen. Ehm, det var faktiskt alla skrivna frågor vi hade. Det gick väldigt mycket fortare än vi hade tänkt.

FS2: Men det var en väldigt givande intervju,

FS1: Ja, verkligen!

FS2: Tack så jättemycket för att du ställde upp.

R1: Inga problem! Lycka till med er C-uppsats!

FS1 & FS2: Tack så jättemycket!

R1: Ha en trevlig dag!

FS1 & FS2: Detsamma! Hej.

Bilaga 3 – Transkribering intervju 2

I följande bilaga kommer det som tidigare benämnts scenario refereras till som casefrågor.

FS1: Ja så då skulle vi vilja börja med att fråga dig X, vad är det du arbetar med? Vad är din roll i verksamheten?

R2: Hej, jag heter X, jag har arbetat på Organisationen i typ 10 år och de senaste typ 3-4 åren på just denna avdelning. Eh jag är... Nu har jag väl rollen kan man säga som en fullstack utvecklare i huvudsak, så det är utveckling i alla led.

FS1: Mm, och...

FS2: Intressant.

FS1: Ja, verkligen. Och alltså vilka aktiviteter då är du med i, är du med i liksom hela livscykeln av systemet eller är det någon speciell del där du kommer in?

R2: Eh nä alltså det är ju väldigt mycket hela så att det är ju... Det inkluderar ju bland annat att man sitter i kanske arbetsgrupper och med projektgrupper med projektledare och planerar hur man ska lägga upp arbete, skissa på lösningar… Alltså mer konceptuellt på ett större plan, men också sen när man kommer till gränssnittet och hela den delen och diskutera och så, så att det… Det skiljer sig såklart, men i flera av de projekten jag varit inblandad i så är jag med i ett väldigt tidigt skede... Ett stöd till projektet innan man ens har börjat prata teknik nödvändigtvis.

FS1: Ja, okej! Yes, hur skulle du säga att den typiska…

FS2: Skulle du kunna…

FS1: Ja, förlåt [skrattar].

FS1: [skrattar] Skulle du kunna beskriva en typisk arbetsdag?

R2: Eh... ja [skrattar], det är ju väldigt olika men eh… Exempelvis igår så… Vi har också... En annan sak jag håller på med löpande är att hantera inkommande ärenden. Nyutveckling är en del men också hantera inkomna ärenden på befintliga system. Och då handlar det delvis om det kommer in förändringsönskemål men också när det kommer in vad som heter incidenter och det är att någonting gått fel, någonting är tokigt. Så att igår var det lite panik, då var det ett stort system som hade gått ner visade det sig och sen så visade det sig att det var flera system som hade gått ner när vi tittade lite på det. Så fick vi laga det helt enkelt så att det funkade i den rollen var jag inne och höll på med certifikat på servrar och ändrade i kod. Och ja, i övrigt så höll jag också på att skriva… Skriva kod i angular typescript för hantera det administrativa verktyg som används i Canvas som jag byggt.

FS1: Ah okej, spännande, hur... Alltså hur ser ett sånt, alltså typ ett förändringsärende, vad skulle det kunna vara, vad är det för förändringar de oftast vill ha?

R2: Ehm, ett förändringsärende det är ju väldigt olika, hur man ska säga, hur avancerad beställarorganisationen är. Ofta i praktiken... Det är ju tänkt att beställarna ska veta, de som äger ett system… Vi använder en ITIL-modell på Organisationen, det är alltså en förvaltningsmodell med systemförvaltare och systemägare, teknisk systemförvaltare och så vidare. Och det innebär... Då liksom finns ansvaren fördelade och där är det ofta den som är systemförvaltare eller någon som tillhör en styrgrupp eller de som faktiskt använder systemen som beställer förändringar. Ofta kanske inte de har den detaljkunskapen om systemet som man hade kunnat tänka sig, eller kunna önska. Utan då är det ju mer luddigt “Ja, jag vill ha…” Till exempel nu fick jag in en förändring vi behöver ändra, nu har vi fått problem med pakethanteringssystemet, det som skickar paket på Organisationen. För att nu har någon lag eller regeländring gjort att det måste vara ändrat när det går utanför Europa och då måste det till någon form av fält någonstans och så. I det fallet så har de kanske inte… De vet ju kanske mycket om postgången, postens rutiner, regler och processer men har ju ingen aning om, alltså vet ju kanske ingenting om det tekniska så att det är mer så “hjälp vi måste lösa det här, vi måste få det att funka utanför Europa” typ.

FS1: Ja…

R2: Och sen får man ju någonstans ha möten, diskutera, vad innebär det här i praktiken? Hur går vi tillväga? Vad blev det för tidsplan? Och lite sådana saker. Också då får jag kommunicera kanske med min chef "okej vad har vi? Vad ligger övrigt i pipen med? Vad blir det med prioriteringar? Om vi gör det här så kommer det ta såhär mycket resurser, det kommer innebära kanske det här arbetet blir lidande istället" och så får det liksom vägas.

FS1: Mm, jag förstår

R2: Medan direkta fel alltid går före, någonting är trasigt ja då fixar man det så fort man kan. Det är en annan process så att säga.

FS1: Ja, precis. Hur jobbar ni med projekt, är det agilt med scrum eller hur brukar det se ut?

R2: Ehm, ja om man ska säga... Det är ju mycket närmare någon form av agil utvecklingsmetod. Men scrum, det är på ett sätt snällt sätt att uttrycka det på, men jag tror att det är ofta är så i utvecklingsprojekt att det är så mycket som kan förändras, så mycket man inte känner till så att det kan bli väldigt agilt, lite kaosartat kanske ibland.

FS1: Ja [skrattar], okej!

FS2: Nästa fråga, hur ser du på personlig integritet i allmänhet? Vad betyder begreppet digital integritet/privacy för dig? Både som utvecklare men också som privatperson.

R2: Alltså, som privatperson så har jag väl bilden av att man är väldigt övervakad, det är väldigt många system som vet väldigt mycket om en och det kan väl ibland vara... Oftast är det inte problematiskt, det är klart att det finns en problematik inbyggd i det och det handlar ju framförallt kanske om när man kanske råkar gå emot en, vad ska man säga, en annan… Ursäkta jag tänker lite, försöker uttrycka mig… Jag vet inte riktigt hur jag menar… Det finns ett scenario nu när man kan få inreseförbud i USA beroende på vad man har skrivit på sociala medier. De tittar igenom sociala medier och ser vad du har skrivit. Om du skrivit något som har klassats liksom som olämpligt så kan du inte resa in. Det tycker jag är en obehaglig utveckling och så är det väl globalt att det finns en möjlighet att följa människor på ett väldigt detaljerat sätt. Det nyttjar jag också privat när jag ska köpa en begagnad bil till exempel, då kollar jag upp dem människorna och vet väldigt mycket om dem… På ett lite stalkeraktigt sätt [skrattar]... För att det är ju så enkelt att göra. Så visst är det så att man måste vara medveten om det då, att man är övervakad kanske man inte kan säga, men att det finns mycket information att hämta och det kan vara problematiskt. Yrkesmässigt får jag att stöta på den här typen av hantering ganska ofta eftersom jag kommer åt en hel del system där det är ganska… Där det är viktigt att det hanteras rätt. Då handlar det om... Exempelvis har jag jobbat med… Nu ett bokningssystem för medicinska studier där barn är inblandade. Då ska man ju inte gärna slarva med dem uppgifterna givetvis och det är viktigt att dem inte kommer ut eller att de även... Och där kan det till exempel ställa till med utmaningar i testning till exempel när… Hur ska vi ha testdata som är riktig när vi inte vill ta produktionsdata… Finns lite överväganden där. Jag har också hanterat nyligen uppgifter om avstängda studenter från Ladok som ska… Där var ett system som behövde ta hand om dem på ett rätt sätt och då är det klart att då måste jag hantera det på ett… Försöka resonera runt det för mig själv att okej någonstans tänka "jag måste undvika att… Hur gör jag för att säkerhetsställa att jag inte slarvar med de här uppgifterna?"

FS2: Hur brukar du då göra för att det ska gå bra liksom, hur brukar du tänka kring det?

R2: Eh, ja… En allmän försiktighet, jag menar det är klart det finns… Jag har skrivit på avtal när jag blev anställd om att man får inte sprida data, givetvis. Men det handlar ju mer om det moraliska att försöka hitta praktiska rutiner för att det ska undvika att spridas. Ett konkret exempel handlar ju om hur man hanterar testdata, att inte den råkar… Att testmiljöer och sånt där är det väldigt enkelt att produktionsdata råkar hamna i en äldre kopia till exempel. Att man är väldigt försiktig med hur den görs, hur den hanteras och hur den exponeras. Där är ju ett konkret exempel när vi har testdata och försöker generera upp den. Det är ju väldigt mycket enklare att bara ta produktionsdata som är gammal, återställa den och jobba utifrån den men att försöka då istället generera testdata… Automatgenerera det, liksom namn, adresser och så va, personuppgifter istället även om det är ett merarbete.

FS1: Ja, precis. Då låter det ändå som du jobbar väldigt mycket med integritet, men är det något du skulle vilja ha ändrat i hur ni på organisationen arbetar med integritet?

R2: Eh ja, alltså lite till sakens natur i och med att vi är en [dolt p.g.a. anonymisering] miljö… då blir det ju mycket persondata som skiftas runt omkring och det kan vara data som också kan vara känslig. Det kan också handla om till exempel data om till exempel avstängningar eller resultat eller från de här medicinska studierna. Det är ju känsliga uppgifter. Där har vi väl… Jag vet inte om… Jag upplever kanske inte ett så aktivt stöd men jag har inte heller efterfrågat det, så jag har svårt att… Det är inget jag direkt kan kritisera. Det är fullt möjligt att det finns ett mer aktivt stöd när man efterfrågar det. Min erfarenhet har varit att i de fallen när vi känner att vi inte riktigt vet var vi ligger juridiskt och rådfrågar jurister då, vilket har hänt vid ett antal tillfällen, då är en jurists standardsvar alltid… De är alltid väldigt, väldigt försiktiga. Så pass försiktiga när man säger vi vet inte hur någonting ska tillämpas och de har alltid någon form av försiktighetsprincip. Och den försiktighetsprincipen är alltid så försiktig så att om man ska tillämpa den så kan man inte arbeta, i princip. För deras svar blir alltid någonstans "det beror på men innan man vet så ska man alltid ta den så att säga striktaste tolkningen" men till exempel då med dataskyddsförordningen och sånt blir det väldigt svårt. Det är ett löpande arbete att göra.

FS2: Kan det vara så att de kanske inte heller riktigt vet så tydligt var gränsen går i och med att lagar kanske är otydliga eller att de kanske inte förstår er tekniska bakgrund och inte kan kombinera det här för att ge ett tydligt svar?

R2: Ja men precis, så är det nog säkert. Också då att rättsfall inte har prövats, vilket ofta är fallet och då har de svårt att säga "ja, vi vet inte". Alltså de har ju inte… Jag menar lagar är ju hur de tillämpas och om de inte har tillämpats eller om man inte har några fall så har de svårt att ge konkreta besked… Men precis som du är inne på, det är klart att det kan också handla om… Det är klart att dem inte har den digitala förståelsen eller vad man ska säga som jurister, att förstå exakt vår roll. Vi kanske inte heller alltid är så duktiga på att kommunicera frågeställningen på ett korrekt sätt.

FS1: Mm. Har ni några etablerade metoder för att identifiera olika risker eller designval som skulle kunna förbättras gällande hanteringen av integritet eller är det mer liksom upp till utvecklaren som sitter med det?

R2: Nja, vi har haft… Vid tillfällen så har vi kört olika såhär test suites för att försöka se om vi ser några säkerhetsluckor och sådana problem. Sen i övrigt handlar det väl också om att hålla saker och ting uppdaterade och använda någorlunda så att säga moderna tekniker. Då får man ju skyddet någonstans inbyggt. Vi är ju mer oroliga för ett gammalt system som bygger på gamla servrar till exempel och där kanske vi tittar en extra gång och sen har vi också en…

Säkerhetsansvariga som kan se om de ser till exempel ovanlig trafik bete sig på vissa sätt. Sen är det också en rutin runtom… Men det är en relativt ny rutin som handlar om man hittar ett fall där information skulle kunna ha läckt ut på något vis. Att det då rapporteras och hanteras enligt vissa rutiner som jag inte har full koll på men det finns en sådan roll numera, men det är klart att det har hänt att information exponeras på olika sätt även om det kanske inte har så att säga… Ingen har kanske uppfattat det men det har funnits tillfällen då skulle kunnat ha kommit ut.

FS1: Mm

FS2: Yes. För vår nästa fråga var lite om ni arbetar aktivt för att uppdatera er med den senaste teknologin gällande integritet, är det något du känner att ni gör?

R2: Alltså, gällande integritet… Nja alltså det handlar ju någonstans om att, exempelvis om man tar ett tekniskt exempel, kommunicerar vi med... Ofta numera försöker vi gå mot de mer moderna moderna sätten att… Ursäkta, nu tappade jag tråden… Vi nyttjar REST-APIer för kommunikation och den informationen som då man kan få ut därifrån den behöver ju… Den får inte läcka ut, utan det är ofta personuppgifter till exempel som kan finnas med i ett svar då och då ser vi till att använda så att säga ny kryptering, nya certifikat, ha ett lösenord som är 24 tecken långt, sådana saker… Alltså för att undvika risker att... Eftersom det är öppet mot internet så undvika risker att någon då kan få ut den här informationen. Exempelvis ett dåligt lösenord hade kunnat leda till att man då skulle kunna söka bland alla anställda och all personal och få ut… Nej alla anställda, alla studenter och få ut deras uppgifter. Mycket av deras uppgifter i klar text. Det hade inte varit bra.

FS1: Nej, såklart!

FS2: Ja.

R2: Så ja, det är något vi tänker på!

FS1: Mm, känner du till begreppet Privacy by Design?

R2: Eh, jag har hört det men… Och jag har läst något om det, men inte så tydligt. Jag har för mig, lite svagt nu att för mig att… För mig såg jag det som att det var svårt att tillämpa det i praktiken på vårt arbete. Att jag liksom därför sorterade bort och inte gick vidare, men inte mer än så.

FS1: Nej, okej!

FS2: Ja.

FS1: Yes! Då tänkte vi gå över till två casefrågor, där du ska få ta lite ställning till olika situationer.

FS2: Yes, jag ska bara ta fram de här sen tänkte jag att jag delar min skärm så att du kan hänga med också. Kan ni se nu?

FS1: Yes! Vill du börja?

FS2: Ja!

R2: Mm!

FS2: Då börjar jag, Tom är en systemutvecklare på ett mjukvaruföretag och han deltar i utvecklingen av ett skräddarsytt program. I projektet finns det en väldigt tydlig arbetsfördelning gällande inloggningsautentisering, verifiering vid betalning, affärsfunktioner…

R2: Ursäkta, för mig är det… Om det är okej så läser jag mycket hellre om det funkar…

FS2: Ja!

R2: Är det okej?

FS2: Ja, absolut!

R2: [Läser caset.] Ehm, jo i det fallet så hade jag svarat ett E. Att jag kommer diskutera den integritetsskyddande strategin med alla involverade för att sedan fortsätta med utvecklingen och implementeringen av den framlagda strategin i det fallet.

FS1: Mm, varför valde du det? Hur tänkte du där?

R2: Ja, nej jag försökte väl lite grann tänka också hur jag har agerat när jag har... Det här är ju svåra frågor som man inte bara tänker på på en sekund [skrattar]. Kan tänka hur har jag agerat i liknande situationer och hur resonerade jag då och då vet jag att när det har varit fall där jag känner att... När det uppfattades som känsliga uppgifter som riskerade att läcka eller jag kände att "vänta nu är det här verkligen rätt i en annan del än vad jag är ensam ansvarig för", i de fallen så lyfte jag det med lite olika personer och det tyckte jag närmast ligger E skulle jag säga.

FS1 & FS2: Mm.

FS1: Och då väntade du med fortsatt utveckling tills ni hade en viss strategi över hur ni skulle hantera det?

R2: Eh… Jag jobbade väl på men vi har ju alltid, alltså produktionssättning är ju en helt annan sak än en utvecklingsprocess så att jag tror väl antagligen att jag jobbade på men att innan någonting sattes i produktion att då hade man rätt ut de delarna.

FS1: Mm.

R2: Så att man pausade inte bara arbetet, det funkar ju inte, det blir ju inte så bra.

FS1: Nej, precis.

R2: Utan man får ju jobba på.

FS1: Mm. Då har vi nästa casefråga.

FS2: Ja, jag ska bara sluta dela. Av någon anledning går det inte att byta slide när man delar… Så, här kommer nästa!

R2: [Läser caset.] Ehm, jo när det gället ett sånt här fall, det var lite lurigare på ett sätt, hade jag gjort punkt B där. Att jag anser att företagets förfrågan kränker användarens

integritetsrättigheter och därför kommer jag ta upp detta med projektgruppen och hoppas på att företaget kan diskutera detta med vår kund först. Jag kommer bara slutföra mitt arbete enligt företagets krav om jag får användarens tillåtelse. Och anledningen till det är väl att… Alltså jag skulle nog tycka generellt att det skulle vara lite illojalt mot arbetsgivaren att berätta för någon utanför utan att det är något annat. Jag tror också att det här tyder ju på ett strukturellt problem som jag hade i så fall… Tycker man i så fall bör lyfta internt att "är det verkligen såhär vi ska göra?". Så jag tror att jag hade gjort punkt B och sen beroende på vad utfallet hade varit hade jag nog funderat på... "är det verkligen här jag ska jobba framöver?"

FS1: Mm, okej! Så du känner att du har vissa skyldigheter både gentemot kunden men också din arbetsgivare? Har jag tolkat dig rätt där?

R2: Nja... Det vet jag inte... Jag vet inte riktigt hur man ska… Om man kan säga ja på det, ehm… Men ja visst har jag ansvar mot min arbetsgivare och sen mot, vad ska man säga, folk i allmänhet. Nä men alltså, om det är just mot den givna kunden eller om det är mot alltså… Någonstans handlar det om en princip snarare om den enskilda liksom... Vad kunden nu kan vara, om det är en privatperson eller om det är ett företag men som... Och att jag tycker då av princip så bör man inte agera på det viset och velat ta upp diskussionen.

FS1: Mm.

R2: Den var lite svår.

FS1: Ja.

FS1 & FS2: Yes!

FS1: Det var faktiskt alla frågor vi hade idag så att vi vill tacka så jättemycket för att ni kom hit och ville svara på dem.

FS2: Det var jättegivande för oss, så tack så jättemycket!

FS1: Tack!

R2: Amen vad bra, lycka till. Jag vet, det är skitjobbigt att skriva uppsats…

FS2: [skrattar].

FS1: Ja [skrattar].

FS2: Tack så mycket!

R2: Lacka inte ur på varandra, det är lätt att göra [skrattar].

FS1: Ja, vi ska försöka låta bli [skrattar].

FS1: [skrattar.] Ja!

R2: Lycka till, ha det så bra!

FS1: Detsamma!

FS2: Tack, hej!

FS1: Hejdå, tack!

R2: Hej!

Bilaga 4 – Transkribering intervju 3

I följande bilaga kommer det som tidigare benämnts scenario refereras till som casefrågor.

FS1: Yes, men då skulle vi vilja börja med att fråga vad är det du arbetar med?

R3: Ja jag är systemutvecklare på avdelningen. Jobbar med utvecklingen av till exempel Canvas, Passport och Epic.

FS1: Ja, är det liksom frontend, backend, fullstack?

R3: Det är fullstack.

FS1: Fullstack, yes.

FS2: Skulle du kunna beskriva lite av de aktiviteterna du sysslar med eller hur en normal arbetsdag ser ut?

R3: Ja… En normal arbetsdag börjar väl med att man kontrollerar vårt felanmälningssystem, vårt ärendehanteringssystem, kollar e-posten och ser om det är incidenter som påverkar den dagliga driften. När man har tagit hand om de fel som kan finnas så går man ju över och kollar i de olika projekten om man har någonting som man kan fortsätta med, något ärende.

FS2: Ja.

FS1: Har du något exempel på fel som kan finnas, alltså är det något som är vanligare än det andra eller?

R3: Nej, det kan man inte säga. Det är högt och lågt.

FS1: Yes. Hur ser du på personlig integritet i allmänhet, alltså vad betyder begreppet digital integritet för dig?

R3: Eh, ja… Vad ska man säga om det… Vi... Jag har ju också läst... Jag har läst på LTH. Vi har också diskuterat personlig integritet i samband med utveckling och man diskuterar väldigt mycket teoretiskt om vad som skulle kunna hända men när det gäller att arbeta på Organisationen så känner jag inte att det kommer så mycket personlig integritet tillsammans med systemutvecklingen.

FS2: Mm… Jag tänker ser du olika på det när du sitter som en utvecklare och sen när du är som användare? Har du olika syn på personlig integritet eller är det något speciellt du tänker på när du som privatperson använder tjänster? Och om det sen är någonting du tänker extra mycket på som utvecklare i yrket när du jobbar?

R3: Nej, det tror jag nog faktiskt inte.

FS2: Nej.

FS1: Så, då skulle du säga att det finns inte så mycket i ditt arbete, alltså integritet?

R3: Nej, tyvärr inte [skrattar] kan man väl säga.

FS2: Hade du velat att det var annorlunda?

R3: Nej, det är rätt så skönt att slippa fundera på personlig integritet när man är utvecklare faktiskt.

FS1: Varför känner du så?

R3: Nja, alltså jag känner ju alltså att ska man ta hänsyn till massa sånt och ha de funderingarna, det är ju jobbigt känner jag.

FS1: Blir det jobbigt för att det blir mycket arbetsbelastning eller hur tänker du?

R3: Nej, det är väl mer psykiskt att behöva tänka på det, det är väl mer psykiskt… Nu slipper man ju fundera på det. Oftast så med våra system är där ju redan någon som har tänkt igenom detta innan det har kommit till oss.

FS2: Då är det ju skönt för er att slippa tänka på det.

R3: Ja.

FS1: Men som fullstack-utvecklare, är du med i hela systemets livscykel eller kommer du in efter ett tag eller… [ohörbart].

R3: Ehm, det är lite olika på olika system. Det finns system där man har varit med redan från början vid första kontakt med kund och varit med i kravställningar och liknande. Och det finns system som efter utvecklingen, som vi sköter driften på.

FS2: Känner du till begreppet Privacy by Design?

R3: Ehm… Känner till det, ja. Vet inte riktigt vad det innebär [skrattar].

FS2: Nej, men det är ingenting ni använder? Det är sju principer som används, eller är tänkt att man ska använda för att bevara personlig integritet och det handlar om sådant som att arbeta proaktivt, bädda in integritet i designen och lite liknande.

R3: Nej, vi jobbar inte efter det, det kan jag väl säga.

FS2: Okej, yes.

FS1: Men har ni några etablerade metoder för att identifiera olika risker eller designval som skulle kunna förbättras gällande just hanteringen av integritet eller personuppgifter?

R3: Nej, det kan jag nog inte säga. Det har vi nog inte.

FS1: Nej, så det är lite upp till utvecklaren själv eller?

R3: Ja, alltså… Vi har ju inte så mycket som rör den personliga integriteten i våra system för om våra system hanterar någon personlig data så är det ju för att vi behöver det och då är där inte så mycket att fundera på.

FS1: Nej…

FS2: Så ni brukar inte ifrågasätta varför just den här datatypen används eller så utan det är redan genomtänkt från andra parter?

R3: Ja det får jag nog säga. Det är väl snarare i så fall att man försöker hindra exponering av personlig data om det inte behövs.

FS2: Har du något exempel på där ni gjort det, eller behövt göra det? Hur har ni hanterat det då?

R3: Vi har ju haft en del, jag vet inte om det faller inom personlig integritet men… Anonymitet, inom till exempel [dolt p.g.a. anonymisering] och sånt här och då har vi ju fått bygga saker så att det blir anonymt så att studenterna får ett id istället.

FS2: Och då bygger ni tekniska lösningar till det?

R3: Då bygger ju vi tekniska lösningar och vi ser allting men när det exponeras för lärare så blir det anonymt.

FS2: Ja.

FS1: Precis. Ehm… Ja, då…

FS2: Har vi några andra frågor eller ska vi kolla på casefrågorna FS1?

FS1: Vi kan nog kolla på casen tänker jag.

FS2: Ja. Vi har två stycken case också som vi tänkte presentera för dig. Jag ska dela min skärm bara.

R3: Mm.

FS2: Så. Kan ni se nu? Nej, du måste godkänna tror jag…

FS1: Ja, gud, förlåt. Så.

FS2: Yes. Kan ni se nu?

FS1: Inte än.

R3: Nej.

FS2: Så. Yes, jag vet inte om du föredrar att läsa själv eller om vi ska läsa upp frågan själv?

R3: Nej, jag läser nog gärna själv.

FS2: Ja, absolut.

R3: [Läser caset.] Ja, det var ju en intressant sak. Och där hade jag ju svarat E.

FS1: E. Varför valde du det?

R3: Ja, alltså detta är ju ingenting som man tar ett beslut på själv. Man måste ju prata om det med de involverade anser jag.

FS1: Känner du att det är viktigt att ha en strategi för hur man ska angripa det också innan man kommer allt för långt...

R3: Det tycker jag nog. Beroende på hur man väljer att angripa det så kommer ju lösningarna till att se väldigt olika ut. Så det är någonting man måste ha med redan från början.

FS2: Yes. Vi har en casefråga till. Så.

R3: [Läser första meningen av caset.] Samma sak men nästan inte, eller?

FS1: Den börjar på samma sätt.

FS2: Den börjar på liknande sätt.

R3: [Läser caset.] Mm… Här beror det ju väldigt mycket på vad man… I vilken situation man sitter i, tycker jag.

FS2: Kan du ge något exempel på någon viss situation du kan koppla till något svar kanske?

R3: Ehm… Alltså här är ju två… Frågan är om man är anställd. Nu ska vi se här han är systemutvecklare på ett mjukvaruföretag… Sitter man där som konsult eller sitter man där som anställd kan ju ha stor betydelse.

FS1: Anställd, tänker jag.

FS2: Men det kan vara intressant att höra din åsikt gällande konsulter också.

FS1: Absolut.

R3: Alltså är man konsult har man ett lite större ansvar och oftast så kan de ju då… Om man skapar någonting som konsult så kan ju hela företaget bakom konsultverksamheten bli ansvarig för en sådan här sak. Samtidigt som man då ofta har konsultchef och liknande i ryggen när man tar beslut. Men jag vet inte om där är något som passar in på det… B… Kanske...

FS2: Du får gärna komma med ett eget förslag också om du känner att du hade agerat på något sätt som du inte kan finna stöd för i svaren.

R3: Ja, alltså, om det nu är ett kryphål så är det ju definitivt att företagets förfrågan kränker användarens integritet, men då tar man ju upp det med företaget först. Man vill ju inte involvera kunden… Man vill ju ändå tänka på företaget, samtidigt så att bara följa instruktionerna och slutföra arbetet känner jag inte heller är aktuellt. Så som konsult hade man ju tagit upp det med företaget först och berättat för dem att det här är inte riktigt rätt. Vill de fortfarande ha det genomfört så går man ju till sin konsultchef och berättar att “jag är inte riktigt bekväm i att göra det här”. Och så får man råd från sin konsultchef då och det… Då

kan man ju fortfarande bli tillsagd att följa företaget. Och då får man ju ta sitt eget beslut beroende på hur allvarlig den här affärsinformationen är, skulle jag vilja säga.

FS1: Absolut.

R3: Jag tycker ju att A är helt förkastligt. E tycker jag också är förkastligt.

FS1 & FS2: Mm.

R3: Men jag tycker B passar bäst faktiskt, om det är… Speciellt eftersom ni skriver att det är ett kryphål så tycker jag nog B är det som passar in mest.

FS2: Ja, jättebra. Det var vårt sista case.

R3: Ja.

FS2: Jag tror vi är ganska nöjda om du inte har något att tillägga?

FS1: Nej, det känns som vi täckte mycket på väldigt kort tid.

FS2: Ja, det var en väldigt givande intervju. Tack så jättemycket för att du tog dig tid.

FS1: Ja, verkligen.

R3: Det var så lite så.

FS2: Tack, du får ha en jättefin dag. Hej.

R3: Tack detsamma, hej.

FS1: Hej.

Bilaga 5 – Transkribering intervju 4

I följande bilaga kommer det som tidigare benämnts scenario refereras till som casefrågor.

FS2: Då kan jag börja med att fråga, vad är det du arbetar med? Och vad har du för roll i verksamheten, skulle du kunna beskriva det?

R4: Ehm, jag har en liten delad roll just så att jag jobbar som typ 50% som utvecklare och 50% som chef, alltså gruppchef, över ett gäng utvecklare som jobbar med den externa webben och applikationerna runtom där.

FS2: Kul. Kan du beskriva hur en arbetsdag ser ut ungefär? Hur börjar din dag, och hur brukar den sluta?

R4: Ja… Man sätter sig vid datorn och kollar så att det inte har hänt några större olyckor och [skrattar] så att alla viktiga siter är uppe och att det inte hänt någonting. Sedan... Jag brukar

börja ganska tidigt, jag börjar redan vid 7 sen har vi inte morgonmöte förrän vid runt cirka kvart i 9. Så då brukar jag titta lite på utvecklingsbrädet, vad vi behöver göra, vad som är på gång och sen så börjar jag jobba på de ticketarna som är på gång eller testar någon annans kod som andra vill titta på. Sen vid 9, kvart i 9, så har vi som morgon-stand up där vi stämmer av med varandra vad vi gjorde igår, vad vi ska göra idag. Ja, sedan så om man behöver hjälp av någon. Det är de tre punkterna man ska köra när vi kör stand up. Och sen så brukar det vara lösa problem, utveckla koden eller prata med folk som har problem eller vara i möten man behöver vara med i, prata med kunder om olika ärenden och diskutera utvecklingsfrågor. Så flyter det på hela dagarna. Ibland blir det kriser och någonting kraschar, då får man gå in och paniklösa det.

FS1: Men jag tänker du…

FS2: Har ni morgonmöte varje dag?

R3: Ja, vi har varje dag. Kvart i 9 så har vi typ 5-minutersmöte. Nu sitter ju alla hemma så nu kopplar vi upp oss på Zoom och tar ett snack. Inte på Zoom, vi använder Teams istället, Microsoft's variant. När jag var på kontoret så hade vi stand up, om ni har läst om agil... Om scrum, så är vi lite så scrum-inspirerade så jag kör stand up, så stående möten för att det inte ska ta så lång tid. Så de ska ju ta runt 5-10 minuter, inte mer än 10 minuter, alla tar bara de här tre punkterna som jag sa.

FS2: Ja. Min nästa fråga var då om ni är scrum-inspirerade, som ni då är?

R4: Ja. Vi kör väl inte scrum helt och hållet men vi har delar av det. Inte helt strikt scrum i processen. Vi tar det vi gillar [skrattar].

FS2: Ja, naturligt att göra så [skrattar].

FS1: Exakt. Jag tänkte lite du sa din roll var lite så 50/50 utvecklare/gruppchef. Vad är det för typ av utvecklare då? Är du frontend, back-end, fullstack?

R4: Ehm… Det har blivit mest back-end och även DevOps så har jag hållit på med en hel del, alltså utvecklingsmiljön och våra servrar på sista tiden. Men det blir i huvudsak back-end och… Jag gör även en del frontend också, så det är lite av varje som behövs.

FS1: Yes. Och din roll som gruppchef, vad är det den innebär? Alltså, vad gör du?

R4: Alltså jag har en väldigt liten grupp, jag har personalansvar för mina 5 utvecklare. Så jag leder ju arbetet helt enkelt… Leder och fördelar ju arbetet och har utvecklingssamtal och lönesamtal och sådant som behövs.

FS1: Så det är du som delar in dem i roller och vad de ska göra i….

R4: Ja. Vi har ju [ohörbart] sen ganska länge så de har ju olika roller. Jag hörde att ni pratade med [dolt p.g.a anonymisering] exempelvis. Han är ju vår frontend specialist, så han tar ju huvuddelen av frontend-frågorna. Sen har vi andra som jobbar med back-end, sök och så vidare. Som har det som specialitet men alla kan in och jobba inom i stort sett allting. Man behöver... Eftersom vi är en så liten grupp kan vi inte specialisera oss helt och hållet liksom. Vi måste överlappa varandra och kunna varandras frågor.

FS1: Mm.

FS2: Ja. Om vi går in mer på integritet, personlig integritet. Hur ser du på det i allmänhet? Vad betyder begreppet digital integritet/privacy för dig?

R4: Ja… Det är ett svårt ämne. Väldigt viktigt på nätet och liksom ja… Integriteten på nätet är väl inte särskilt stor tycker jag, om man inte verkligen jobbar efter att skydda sig ordentligt. I stort sett allt du gör ser Google liksom, Google vet säkert mer om mig än vad jag vet. Så att ja… [Ohörbart.] Jag är inte manisk att, ja, skydda min integritet. Jag känner en del utvecklare som är sådana, alltså riktiga Linux-nördar, som tycker att man inte alls ska ha någonting med Google och göra för att de bara trackar en liksom så att… Så är jag inte alls utan jag använder Google-produkter och då får man på något sätt acceptera… Och andra, typ Facebook och så då får man ju accepetera att…

FS2: Att det är så det är!

R4: Att det är så det är liksom. Tyvärr. Jag gillar det inte men jag ser inte riktigt någon… Jag vill ju också ha de här gratistjänsterna som Gmail och Google Docs och allt det här liksom.

FS2: Det är ju den delen som är lite jobbig. Man vill ha det men... Det blir lite svårt att leva utan det nu också.

R4: Ja, visst. Man kan ju, men man får betala, [ohörbart] eller göra det själv. Men det blir ju jobbigt.

FS2: [skrattar] Ja, det kan man också göra. Min nästa fråga tog du upp lite här nu men ser du på det på olika sätt som användare och sen som utvecklare? Har du olika syn när det kommer till integritet?

R4: Alltså som utvecklare får man ju tänka på vad man själv gör och inte kränker andras integritet. Där accepterar jag ju inte att man beter sig som Google i våra produkter. Då måste vi ju vara väldigt varsamma och följa GDPR och nästan liksom… Med allt sådant vara väldigt noggranna, men det är ju en... Lagstiftningen på det här området är ju en djungel, så det är jättesvårt och veta ifall man gör rätt. Jag har varit på utbildningar och sådär och det är ju ingen som riktigt vet vad det är man ska göra för något för att göra rätt, än så länge. Det kommer väl nog reda ut sig, men just nu så är det väldigt snårigt.

FS1: Så du känner…

FS2: Det var någon…

FS2: Så du känner att det finns en brist på ramverk och riktlinjer för hur man ska hantera integritet?

R4: Alltså ramverk finns ju miljoner, det finns jättemycket kod… Inte kod, utan lagstiftning som säger olika och såhär men det finns inte riktigt… Det är de här ramlagarna. Sen så behövs det ju exakt… När vi sitter på en detaljerad nivå, vad är det som egentligen gäller? Och hur ska det hanteras? Där behövs det mer riktlinjer liksom, inte bara riktlinjer utan konkreta exempel.

FS1: Mm. Att det kan vara lite svårt att omsätta i praktiken liksom?

R4: Ja.

FS1 & FS2: Mm.

FS2: Vi pratade med någon som sa att ni ibland tog hjälp från jurister, men att ni inte alltid kände att de heller riktigt kunde ge bra svar. Stämmer det?

R4: Ja, jo, det stämmer ju för mig också. Juristerna vet ju inte heller. Alla går och väntar på att det ska komma några domar… Jag vet inte ifall ni har hört talat om den här Schrems.

FS1 & FS2: Nej.

R4: Det är en lag som, eller en dom, som kom i somras om att man inte får föra över personlig data till USA längre.

FS1 & FS2: Mm, okej.

R4: Och den är också såhär jättesvår att hantera. Vad är "föra över data"? Det är lite osäkert såhär, får man använda… Eller är det tillåtet att föra över det till företag som är amerikanska så även om de inte är i USA får man inte föra över det och såhär… Det är väldigt osäkert vad det är som egentligen gäller. Det är samma med cookie-lagen, vad är egentligen cookies som man ska berätta om? Exempelvis, vi har problemet på organisationens hemsida exempelvis. Vi har ju massa redaktörer. Om de bäddar in en massa material från YouTube eller Google, då kommer det ju in andra applikationer, tredjepartsapplikationer, som ger kakor och lite sådär. Och där blir det ju också lite luddigt, vem är det som ansvarar för vad etc. Det är väl så att det kanske inte riktigt är okej att det görs saker som blir lite fel ibland.

FS2: Vad skulle du säga kan göras i nuläget för att underlätta arbetet för er? Behövs det tydligare lagstiftning eller..

R4: Ja, det behövs tydligare, inte lagstiftning... Kanske mindre lagstiftning [skrattar] på området. Men det skulle behövas, om man ska veta hur man ska hantera den lag som finns skulle det finnas konkreta exempel på vad det är som är tillåtet och inte liksom, efterfrågar jag. På den här Schrems så var jag på en utbildning där det var ett gäng jurister som pratade om det, men de satt ju bara och spekulerade liksom om vad det är som egentligen gäller men att vi får se när det kommer till domar och så. Och jag tror att det på många områden där exempelvis GDPR hanteras så är det så att det är väldigt få som riktigt vet hur man ska hantera detta.

FS2: Känner du att det är svårt att kommunicera med jurister ibland för att de kanske inte förstår den tekniska delen/utvecklarsidan?

R4: Det är väl mer så att jurister är väldigt försiktiga. När de inte vet så vill de ju inte uttala sig och då börjar de prata svepande. Så det är väl mer det som är problemet, att de heller inte vet liksom. Och att det är ingen som vet, och därför så kan de inte vara tydliga helt enkelt. Jag tror att det är det som är problemet.

FS1: Yes. Har ni några policies eller normer för hur man arbetar med digital integritet i era projekt?

R4: Ehm… Alltså… På avdelningen exempelvis har vi väl inte det mer än att vi ska följa lagstiftningen liksom. Och det är ju ganska mycket där liksom. Vi ska ju följa GDPR, leva upp till den lagstiftningen som vi har med GDPR och cookies. Men vi har inga egna skrivna policies om det, vad jag känner till. Det kanske jag har missat [skrattar].

FS1: Skulle du ha velat arbeta annorlunda med personlig integritet? Alltså, att ni skulle ha haft några policies eller att ni arbetat på något annat sätt?

R4: Nej, jag tycker att vi… Alltså, jag skulle vilja vara lite mer säker på att jag gör rätt annars så känner jag väl inte att någon policy hade gett något stöd här utan kan man hålla sig till de reglerna som finns i GDPR så har man ju ganska bra personlig integritet tycker jag. Och att det även räcker rätt långt, att man behöver inte gå utöver det faktiskt, tycker inte jag. Jo, visst, men tydliga regler eller instruktioner på hur man ska följa upp dem, men det är inget vi kan ta fram på organisationen riktigt.

FS1: Nej, såklart.

R4: Mm, tyvärr.

FS2: Arbetar ni aktivt för att hålla er uppdaterade med den senaste teknologin gällande integritet?

R4: Ja… Det gör vi ju… Det försöker vi ju hela tiden att göra, det gäller ju all teknologi men sen så är det ju… Som utvecklare är det ju ett ständigt jobb. Det kommer ni ju märka när ni kommer ut att det ni lärt er i skolan nu kommer inte vara up-to-date i många veckor. Utan alltså, man måste hela tiden hitta, läsa på information och uppdatera sig när man jobbar kring [ohörbart] .

FS2: Är det något speciellt ni gör för just integritetsdelen eller det är allmänt att ni bara försöker läsa på, utvecklas inom...

R4: Det är nog inte något specifikt för just integritet utan vi håller oss uppdaterade generellt och då kommer ju det in. Vad behöver man göra för kakor och hur hanterar man det, då behöver man liksom titta på det lite då och då.

FS2: Ja.

FS1: Känner du till begreppet Privacy by Design?

R4: Ehm… Jag har nog inte läst på om det men det låter som att man ska börja med att ha med privacy när man tänker… När man designar ett system från grunden.

FS1: Ja, exakt. Det handlar om att privacy ska vara liksom inbäddat i hela systemutvecklingsprocessen.

R4: Ja, men det har ju funnits flera såna. Man har ju använt “by design” i flera begrepp innan så att… Men just denna har jag nog inte hört, tror jag inte. Men jag förstår konceptet, att man måste ta med det när man börjar planera ett projekt.

FS1: Ja. Är det något…

R4: Tyvärr är de flesta projekt inte nya som vi håller på med, utan uppdateringar av gamla [skrattar] och utvecklingar av gamla. Det är inte så ofta man får göra ett nytt system som utvecklare. Det är mera sällsynt, lite då och då. Men självklart så är det ju nu med GDPR så är det ju saker som man måste tänka på. Att göra det möjligt och enkelt exempelvis att glömma folk, för det blir ju väldigt jobbigt om man inte bygger det bra. Om man ska rensa ut alla

gamla användare och gjort det på ett klumpigt sätt så… Man biter sig själv i baken om man inte har med den biten från början.

FS2: Nu pratade du lite om det, men har du något projekt som har behandlat personuppgifter på något… Som du kan beskriva lite mer ingående för oss?

R4: Alltså, personuppgifter har vi på webben men vi har nog inte känsliga personuppgifter. Alltså typ, man delar upp personuppgifter i namn, mejladress, ses inte som känsliga personuppgifter. Men till exempelvis personnummer är känsliga uppgifter och vi tar ju ut… Eftersom vi jobbar ju med den externa webben i min grupp och exempelvis om man går in på organisationens hemsida så kan man hitta persondata ifrån anställda om man går in i söken. Och vi jobbar ju med... All den data som vi jobbar med, eftersom vi jobbar med den externa webben, ska ju den visas utåt. Så då får det inte vara känslig data. Så att vi får ju se till att rensa bort känslig data. Vi har en webbtjänst som integrerar emot personalsidan. Så där jobbar vi med persondata och personalsidan är ett system som har... Personalsidan och IAM tror jag det heter som innehåller data från anställda på Organisationen och då får vi se till att vi inte tar ut… Den innehåller ju all data om personalen, där kan vi ju ta ut personnummer och rubbet. Men eftersom vi ska ha det externt på webben så tar vi bara ut det vi behöver där, så det måste man ju tänka på.

FS1 & FS2: Ja.

R4: Så det är väl där vi främst hanterar personlig information i stora mängder.

FS2: Mm. Jag vet inte, har du några fler frågor FS1 eller ska vi gå över till casefrågorna?

FS1: Nej, jag tänker att vi kan gå över till casefrågorna.

FS2: Ja. Vi har två casefrågor som jag tänkte dela här med dig. Kan ni se nu?

FS1: Yes. Det är bara att läsa och ta sin tid.

R4: Ska jag läsa den? Ja. [Läser caset.] Ska man välja en?

FS1 & FS2: Ja!

FS2: Du får gärna säga hur du tänker kring det också.

R4: Ja, A kan man väl säga att man inte riktigt håller med om. Om han jobbar med inloggningsautentisering, verifiering och betalningar i affärssystem kan jag tänka mig att det är en typ av webbshop eller något sådant kanske de håller på med.

FS2: Ja.

R4: Då har man ju mycket både säkerhetsfrågor… Då kommer man att jobba med pengar, kontonummer… Det är ungefär så känsligt det kan bli. Om man inte har sekretess… Säpomaterial och sådant. Och B kan jag heller inte hålla med om då. Ehm… C… Jag kommer ju säkert utföra något arbete så fort som möjligt men jag tror att det är bättre att testa risker tidigare än när allt är fixat. Jag tror nog… Då ska vi se här. D har vi… E är väl det helt klart rätta svaret, jag kommer väl ligga där någonstans mellan D och E beroende på hur bråttom och stressat det är. Men det man skulle vilja göra är ju E, definitivt. Det här är som sagt

väldigt mycket integritet och man behöver mycket skydd. Man måste se till att vara säker och att man har tester och var man gör av data.

FS2: Yes. Då ska jag dela nästa casefråga också. Kan ni se nu?

FS1: Nu.

R4: Där kom den. [Läser caset.] Ja, jag tycker ju inte att det är okej. Men hur skulle jag agera? Det är lite svårt att vara säker på, det beror ju lite på vad man har för finansiell situation i det läget man sitter i. För att det kan ju liksom... Om man inte gör det man ska så kanske man får kicken [skrattar]. Jag hade ju definitivt sagt till företaget att jag tycker att användaren bör känna till detta…

FS1: Du får komma på ett eget svar också om du inte tycker att någon passar.

FS2: Ja, du kan kombinera två svar om du vill!

R4: [skrattar] Ja, okej. Nej men som sagt kanske jag kan välja någon utav de här, vi får se. Ehm… Det är bara någon som ringer på någon annan tjänst om ni hör att det ringer. Eh… Jag skulle ju vilja agera som på B, om jag har ekonomisk möjlighet att ta ett annat jobb [skrattar]. För att det är ju det som kan bli konsekvensen tänker jag.

FS2: Så är det nog. Ja, det var nog allt vi hade tror jag. Stämmer det? Har du något att tillägga?

R4: Nej.

FS1: Nej. Tack för att du tog dig tid!

FS2: Ja vi är jättetacksamma för att du tog dig tid och ställde upp. Det har varit en jättegivande intervju för oss, så tack så jättemycket. Vi önskar dig en trevlig dag.

R4: Ja, hejdå!

FS1 & FS2: Tack, hejdå!

Bilaga 6 – Transkribering intervju 5

I följande bilaga kommer det som tidigare benämnts scenario refereras till som casefrågor.

FS2: Då tänkte jag börja med att fråga vad du arbetar med och vad du har för roll i verksamheten?

R5: Jag jobbar som systemutvecklare på Organisationen, på X heter den avdelningen. Vi… Ja, vi utvecklar och förvaltar alla de applikationerna som både Organisationen och till viss del även andra organisationer i Sverige använder för att… [dolt p.g.a anonymisering]. De flesta systemen är skrivna i Java. Så att jag är javautvecklare och sitter där och gör allt från… Ja vi

gör ju hela liksom… Hela fullstack-delen liksom, från server till gränssnitt, användarvänlighet och så där… Så det är mycket, det är heltäckande liksom.

FS2: Kul. Hur ser en typisk arbetsdag ut? Skulle du kunna beskriva lite?

R5: Eh… Det är ganska standard, vi kan jobba lite som vi vill, eh… Ja vi har flextid, man kommer in när man vill mellan 7 och 9 på morgonen och sen är det ju då ofta upplagt med vilka ärenden som ska göras. Det är ju uppdelat, ibland jobbar man i projekt… Ibland är det liksom förvaltningsdelar eller buggar som har kommit in som behöver fixas. Man tar det, ofta har man ganska bra koll på vad man gör från en dag till en annan. Det är oftast inget jättestort som händer över natten så! Så det är liksom… Det är ganska standard. Man jobbar på liksom och sen är det lunch o sådär. Jobbar man i projekt så har vi ju ofta liksom deadlines eller sprintar och sånt där som man har… Kanske jobbar i tre veckorsperioder eller vad man ska säga och då levererar man något större efter de tre veckorna… Annars så är det liksom… Det löper på bara, man utvecklar vanligtvis och även reder ut krav eller diskuterar med kunder vad som är på gång eller om de har någon liksom fråga eller sådär.

FS2: Kul! Arbetar ni efter Scrum eller?

R5: Sådär… Kan man ju säga [skrattar].

FS2: Scrum-inspirerat kanske?

R5: Ja, de försöker iallafall med lite mera agil utveckling så att det inte är den här vattenfallsmetoden för den har vi ändå konstaterat att det är ingen hit liksom.

FS2: Ja! [skrattar] Det har vi också lärt oss på vår utbildning! [skrattar].

R5: Mm.

FS1: Jag tänker i projekt och så här… Har du ofta en specifik roll då eller är du med lite överallt, i lite olika grejer, eftersom du är fullstack?

R5: Eh... Det är… Vi är lite överallt. Vanligtvis är det ju mest back-end-utveckling men vi måste ju göra frontend-delarna också. Men sen är det ju folk som är mer eller mindre bra på det. Jag håller mig gärna på backend-sidan… Så kan någon annan arbeta med CSS och HTML och sådär liksom, men visst vi gör det också, vi diskuterar även med… Ja men med nätverk så att de öppnar brandväggar så att de kan komma in till applikationerna och sådär. Så det är mycket, det är brett liksom, det är inte liksom "nu ska du koda den här delen" utan man kan ju också prata med kunden för att reda ut vad det är de vill ha ner till hur ska det se ut och hur gör vi detta bäst med liksom det systemet som vi har.

FS2: Kul, låter intressant!

R5: Mm.

FS2: Hur ser du på personlig integritet i allmänhet skulle du säga? Vad betyder begreppet digital integritet eller privacy för dig?

R5: Alltså jag har ju inte funderat så mycket på det. Det kommer ju upp nu med de här… Den här stora frågan som apple ska skicka ut…

FS2: Japp!

R5: Den här att... Det är väl det enda jag tänkt på egentligen. Men man måste inse att vissa grejer… Vill man vara med så måste man offra en del, så är det bara och i Sverige är vi ju ganska... Vi sitter ju ganska illa till, vi har ju personnummer som säger allt om oss och det finns öppet liksom. Så mycket mer personlig integritet… Ja man behöver inte… Har man visat sitt personnummer har man sagt ganska mycket om sig själv.

FS1: Ja, det är sant.

FS2: Skulle du säga att du har olika syn på det beroende på privat användande eller om du tänker ur ett utvecklarperspektiv, när du sitter och utvecklar?

R5: Jag tror jag tänker samma… Lite att man kan inte komplicera system hur mycket som helst för att folk kanske inte vill ange sitt personnummer. Eller om vi… När GDPR var stort så sa de ju att "amen vi kanske vill försöka identifiera folk på ett annat sätt än via personnummer". Det blev jättejobbigt kan jag säga [skrattar]. För att det finns någonting i Sverige som definierar alla väldigt tydligt och det är personnumret, och det är unikt liksom.

FS2: Ja.

R5: Ska man börja med andra grejer… Förnamn, efternamn… Ja det finns någon annan som kan heta samma sak… "Amen om vi lägger till adress"... Ja men det kan ju bo någon på samma adress, måste vi ha liksom trappnummer… Ja det är kanske långsökt att man heter samma sak och bor i samma lägenhet men det går. Personnummer har man liksom inte mer än en person. Jag är väl lite för att man måste ändå hålla det enkelt och då får man offra en del om man vill vara med. Det är ju… När man signar upp för att plugga så har man liksom gett sitt samtycke till att man registreras och så vidare och det liksom får vi ju hålla på. Sen behöver man ju inte spara onödig information, till exempel hur någon har klickat runt och såhär. Det behövs kanske inte för vårt system och då behöver vi inte spara det, men man måste hålla det på den enkla nivån att vi måste kunna… Systemet måste kunna jobba och fungera smidigt och då får användaren offra lite av sin information för att det ska göra det liksom.

FS2: Skulle du säga att det här med personlig integritet och så ibland kan sätta käppar i hjulet för funktionaliteten som systemen kan erbjuda?

R5: Det kan ju göra det, men jag tror inte att vi… Vi råkar inte ut för det så mycket här. Det är inte alla system vi jobbar med heller som har personer utan det är, då är det själva användarna som är inloggade och då är det kanske inte uppgifter som vi behöver spara överhuvudtaget. Men om det är folk som till exempel ska anmäla sig till en kurs, ja då måste vi spara vad den har skrivit för motivering och så vidare. Det är liksom inget vi kan… Vi sparar det av en anledning, vi sparar ju inte saker... Inte på avdelningen sparar vi inte saker för att sälja någonting i framtiden.

FS: Mm.

FS1: Precis! Jag tänker, när du sitter som användare på till exempel Google…

R5: Mm…

FS1: Känner du dig då, vad ska man säga… Bekymrad eller så över hur… För vi vet ju hur mycket data de samlar in om oss.

R5: Mm.

FS1: Hur känner du där?

R5: Nej alltså jag är nog ganska obrydd om sådana grejer. Det har ju kommit upp det här med att "åh man kan bli kategoriserad" och det kan bli fel liksom. Du kanske inte får ett banklån för att du någon gång har sökt på en ärftlig sjukdom eller, alltså… Den här typen av kategorisering och sätta människor i fack, men den kategoriseringen går att göra ändå. Även om det inte samlas in data via dina sökningar till exempel. Så att jag tror… Vi vill ju ha information tillgängligt och gratis och snabbt och då får man liksom offra lite grann. Då köper man det här med att man delar med sig av sin egen information.

FS2: Ja. Känner du till begreppet Privacy by Design?

R5: Nej, inte så…

FS2: Nej, det är ett ramverk som består av sju olika principer för att bevara personlig integritet och principerna hanterar sådant som att arbeta proaktivt och bädda in integritet i utvecklingsstadiet redan, är det något ni tänker på när ni arbetar?

R5: Nej, det kan jag inte säga att vi gör [skrattar].

FS2: Men personlig integritet, finns det i ditt arbete, eller det ingår inte i dina arbetsuppgifter kanske?

R5: Nej, i stort sett inte. Det ingår att vi ska förhålla oss till GDPR och det är… Eftersom vi är en myndighet eller ligger under det här så är det ganska… Vi slipper ganska mycket av det här som kommersiella företag råkar ut för, för att man kan inte välja att radera sina uppgifter hur som helst när man är en myndighet… Alltså när vi är en myndighet liksom.

FS2: Ja.

FS1: Mm.

FS2: Upplever du att det är svårt att följa GDPR eller är det tydligt vad man får och inte får göra?

R5: Ja det är ju lite trixigt, framför allt är det olika… Alla har sin egen definition lite grann. "Får man lov att skriva ett personnummer i en serverlogg", ja säger någon, nej säger någon annan… Ja, det är liksom… Det är lite flummigt. Vi har väl liksom haft massor genomgångar om hur man ska göra och så men folk tolkar olika ändå.

FS2: Vem är det som håller i genomgångarna, är det jurister eller?

R5: Det har varit säkerhetsspecialister är det nog, men det är tekniskt liksom.

FS2: Ja!

FS1: Har ni några etablerade metoder för att identifiera olika risker eller designval som skulle kunna förbättras gällande hanteringen av integritet, eller då GDPR?

R5: Nej, inget sånt.

FS2: Arbetar ni aktivt för att hålla er uppdaterade med de senaste teknologierna gällande integritet?

R5: Nej, det kan jag inte heller säga att vi gör. Vi är nog ganska obrydda tills någon gnäller på oss eller om någon ställer en aktiv fråga just om GDPR till exempel. Annars tror jag inte vi tänker… Det är väldigt mycket administrativa system som… Alltså vi loggar ju inte, vi vill ju liksom inte… Vi säljer ju ingenting så vi loggar ju inte vad någon har köpt till exempel. Utan vill man anmäla sig till en kurs skickar man ju in sina uppgifter eller om man plockar fram ett utbildningsprogram eller så. Det är väldigt… Det är ju inte kommersiellt liksom och det är ju inte… Det är ju väldigt, väldigt administrativt och tråkigt [skrattar] om man ska vara ärlig liksom.

FS2: Ja! [skrattar]

R5: Så vi… det är inte så mycket personuppgifter vi behöver spara eller den typen av grejer.

FS2: Har det hänt att ni ifrågasatt information som kommit in och undrat ifall ni behöver spara just den delen eller så? Eller det går av rutin att det brukar vara rätt uppgifter?

R5: Ja vi försöker ju… Om vi utvecklar nytt, så försöker vi ju se "behöver vi den här", "behöver vi telefonnummer" liksom. "Ja, nä, jo, nä men kanske, någon kanske behöver den någon gång" ja men då… Om det är liksom en kurs och 250 som behöver ringa sina, så kanske de kan skriva det någon annanstans eller så. Då behöver vi inte spara telefonnummer på alla till exempel.

FS1: Känner du att du skulle vilja arbeta annorlunda med integritet eller hur ni förhåller er till GDPR, skulle du önska att det var på ett annat sätt?

R5: Ja, alltså just de här klara riktlinjerna kunde ju ha varit lite klarare [skrattar] än vad de faktiskt är, det hade ju varit en fördel, men sen… Jag tror ändå att vi tänker att vi sparar och använder bara det som vi precis behöver för att systemen ska fungera liksom.

FS2: Du som utvecklare, vad känner du att man behöver göra för att de här sakerna ska bli tydligare?

R5: Alltså, någon måste ju reda ut det, och inte reda ut det för sin egen… Ur sitt eget intresse. Så om en utvecklare som är intresserad av de här frågorna gör en sån utredning så tror jag den blir mycket mer omfattande än om någon som inte riktigt bryr sig gör det. Så vi skulle ju behöva ha någon mer samlad bild, uppifrån alltså, chefer och så här. För man kan ju säkert lägga hur mycket tid och energi som helst på detta, men det är inte säkert att våra kunder vill betala för det heller till exempel [skrattar].

FS2: [skrattar] Ja! Det blir ju lite så om kostnaderna ökar också så är det kanske inte lika… Precis som vi gillar att använda Google för att det är gratis så kan det vara lite så hos de också.

R5: Mm, precis!

FS2: Ja… Jag vet inte FS1 om du har fler frågor eller om vi ska gå över till casefrågorna?

FS1: Nej, vi kan nog gå över till casefrågorna tänker jag!

FS2: Ja, vi har två casefrågor också som jag tänkte dela här med dig.

R5: Mm.

FS2: Ett ögonblick bara! Kan ni se de nu?

FS1: Ja!

R5: Japp.

FS2: Jag vet inte om du föredrar att läsa själv eller om vi ska läsa upp det?

R5: Jag kan läsa. Nu ska vi se här…

FS2: Jättebra!

R5: [Läser caset.] Oj, eh… [skrattar]... Nu ska vi se här… Alltså ja, gud… Jag tror, alltså hade det varit jag så hade jag nog valt D ehm…

FS1: Okej… Vill du…

R5: Jättesvårt…

FS1: Skulle du vilja motivera…

R5: Ja, det är jättesvårt… Eh… Det är ju, för alltså oftast… Man diskuterar ju ofta lite grann men kanske inte med alla involverade… Åh, det är jättesvårt… [skrattar]

FS2: Men du får komma med egna förslag också om du känner att du kanske vill kombinera något svarsalternativ med något.

F5: Alltså, D och E hade ju nog varit att man diskuterar ihop med någon i projektet och sätter upp en strategi och sen så fortsätter vi. För ofta är det ju inte min del som utvecklare i alla fall att göra de här kritiska säkerhetstesterna och så men man kan ju ändå påpeka det liksom.

FS2: Ja… Då ska jag ta upp den andra casefrågan också. Här har vi den.

R5: [Läser caset] Ehm… Ja… C skulle jag nog säga.

FS1: Mm. Varför kände du C?

R5: Amen… Ja, jo… Det är nog ändå viktigt att informera om vad det är man samlar in. Sen behöver man kanske inte gå i detalj på vad det är för någonting, men har man sagt att man samlar in data så… Ja det hade man ju uppskattat liksom. Sen är de ju ingen som läser de varningarna iallafall liksom. Att nu spara vi hur mycket som helst om dig "Ja, enter, jag godkänner", men då har man ju berättat liksom. Och då är det liksom… Om det hade läckt sen från företaget till exempel så är det ju inte ens eget fel, lite så att man har inte samlat in bakom ryggen på användarna.

FS2: Ja.

FS1: Nej, precis. Men du känner inte att du vill ta upp det med arbetsgivaren först eller? Du hade gått till kunden direkt?

R5: Ehm… Men, är där en sån? Nu ska vi se här…

FS1: Ja, B är ju lite mer att man först pratar med företaget.

R5: Eh ja… Men bara för… Ja… För jag tänkte ju att C, det var ju liksom ingen tillåtelse från kunden utan man kan ju bara sätta upp en lapp om att "vi kommer att spara den här datan, så vet du det" liksom. Eller en notis på något vis. För då är det underförstått att går man vidare så har man godkänt det, medan B tänker jag mer att det måste specificeras ordentligt men ja, kanske B istället då. Just att helst diskutera så att alla i projektet tycker samma sak är ganska viktigt annars kommer någon att lösa det på egen hand om företaget trycker på iallafall liksom.

FS1 & FS2: Mm.

FS1: Toppen!

FS2: Jättebra! Tack så jättemycket! Eh… Jag vet inte FS1 om du har något att tillägga?

FS1: Nej det var nog alla frågor vi hade faktiskt, de blev avklarade snabbt!

FS2: Yes!

R5: Mm.

FS2: Tack så jättemycket för att du tog dig tid!

R5: Ja, det är ingen fara, jag har inte tänkt på det här så jättemycket, det kanske inte är så uttömmande svar liksom [skrattar].

FS2: Jo, jag tycker ändå det var givande, vi har intervjuat några stycken så det är kul att jämföra och se hur alla ser på det!

R5: Ja, det finns alltid de som är otroligt insatta i detta och bryr sig väldigt, väldigt mycket, och jag är inte det men [skrattar].

FS2: Men det är kul att man har med båda då så…

FS1: Vi får en bra inblick i det hela.

R5: Mm.

FS2: Så vi tackar för oss och önskar dig en trevlig helg!

R5: Ja, tack detsamma!

Referenslista

Abrams E, M., Cavoukian, A. & Taylor, S. (2010). Privacy by Design: essential for organizational accountability and strong business practices. Tillgänglig online: https://link.springer.com/content/pdf/10.1007/s12394-010-0053-z.pdf [Hämtad 8 april 2021]

Ahmadian, A., Strüber, D., Riediger, V. & Jürjens, J. (2018). Supporting privacy impact assessment by model-based privacy analysis, SAC '18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1467-1474. Tillgänglig online: https://dl.acm.org/doi/pdf/10.1145/3167132.3167288 [Hämtad 9 april 2021]

Ayalon, O., Toch, E., Hadar, I. & Birnhack, M. (2017). How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate, CSCW '17 Companion: Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, pp. 135-138. Tillgänglig online: https://dl.acm.org/doi/abs/10.1145/3022198.3026326 [Hämtad 7 april 2021]

Bryman, A. (2016). Samhällsvetenskapliga metoder, Stockholm: Liber.

Bu, F., Wang, N., Jiang, B. & Liang, H. (2020). "Privacy by Design" implementation: Information system engineers' perspective, *International Journal of Information Management,* vol. 53, 102124. Tillgänglig online: https://www.sciencedirect.com/science/article/pii/S0268401219308606 [Hämtad 8 april 2021]

Cavoukian, A. (2009). Privacy by Design - The 7 Foundational Principles [pdf]. Tillgänglig online: https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf [Hämtad 6 april 2021]

Doffman, Z. (2021). Do You Suddenly Need To Stop Using Facebook?, Forbes, 9 maj. Tillgänglig online: https://www.forbes.com/sites/zakdoffman/2021/05/09/this-is-why-you-should-delete-facebook-on-your-iphone-ipad-android-pc-or-mac/?sh=1b546b7e7b3d [Hämtad 10 maj 2021]

Europeiska kommissionen. (n.d. a). Vilka huvuddrag i den allmänna dataskyddsförordningen ska en offentlig förvaltning känna till? Tillgänglig online: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-dat [Hämtad 10 maj 2021]

Europeiska kommissionen. (n.d. b). Måste mitt företag/min organisation ha ett dataskyddsombud? Tillgänglig online: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_sv [Hämtad 10 maj 2021]

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S. & Balissa, A. (2018). Privacy by designers: software developers' privacy mindset, *Empirical Software Engineering*, vol. 23, pp. 259-289. Tillgänglig online: https://link.springer.com/article/10.1007/s10664-017-9517-1 [Hämtad 12 april 2021]

LeCompte, M. & Goetz, J.P. (1982). Problems of Reliability and Validity in Ethnographic Research, *Review of Educational Research*, vol. 52, no. 1, pp. 31-60. Tillgänglig online: https://www.researchgate.net/publication/255615696_Problems_of_Reliability_and_Validity_in_Ethnographic_Research [Hämtad 11 maj 2021]

Lessig, L. (2009). Code 2.0 [e-bok] New York: Basic Books. Tillgänglig online: https://books.google.se/books?hl=en&lr=&id=tmE-pvNIX38C&oi=fnd&pg=PR2&dq=lessig&ots=Gc0zkJqABc&sig=IfySkSbgoOk1lettWEaE0ef8pe8&redir_esc=y#v=onepage&q=lessig&f=false [Hämtad 14 april 2021]

Martin, Y-S., del Alamo, J. & Yelmo, J. (2014). Engineering Privacy Requirements Valuable Lessons from Another Realm, *IEEE Workshop on Evolving Security and Privacy Requirements Engineering,* pp. 19-24. Tillgänglig online: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6890523&casa_token=rIDUdqDWSNEAAAAA:o5cAuSIKLaIp-qBzDIltbOQdTeSvSTrjF9nNaTbx-IFYD5Nheqlkgv9ZRsnRS9Air2PIBtqM-CQ [Hämtad 16 april 2021]

Mehrpour, S., LaToza, T. & Kindi, R. (2019). Active Documentation: Helping Developers Follow Design Decisions, 2019 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC). Endast sammanfattning. Tillgänglig online: https://ieeexplore.ieee.org/document/8818816 [Hämtad 15 april 2021]

Nationalencyklopedin. (n.d. a). Dataskyddsförordningen. Tillgänglig online: https://www.ne.se/uppslagsverk/encyklopedi/lång/dataskyddsförordningen [Hämtad 8 april 2021]

Nationalencyklopedin. (n.d. b). Reliabilitet. Tillgänglig online: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/reliabilitet [Hämtad 26 april 2021]

Recker, J. (2013). Scientific Research in Information Systems: A Beginner's Guide, Berlin: Springer. Tillgänglig online: https://link.springer.com/content/pdf/10.1007%2F978-3-642-30048-6.pdf [Hämtad 12 maj]

Rienecker, L. & Jørgensen, P. (2014). Att skriva en bra uppsats, Stockholm: Liber

Senarath, A. & Asanka, N. (2018). Understanding user privacy expectations: A software developer's perspective, *Telematics and Informatics*, vol. 35, no 7, pp. 1845-1862. Tillgänglig online: https://www.sciencedirect.com/science/article/abs/pii/S073658531830296X# [Hämtad 14 april 2021]

Spiekermann, S. (2012). The Challenges of Privacy by Design, *Communications of the ACM*, vol. 55, no. 7, pp. 38-40. Tillgänglig online: https://www.researchgate.net/publication/254004794_The_Challenges_of_Privacy_by_Design [Hämtad 8 april 2021]

Wright, D. & De Hert, P. (eds.). (2012). Privacy Impact Assessment [e-bok] Berlin: Springer Science+Business Media. Tillgänglig online: https://books.google.se/books?hl=en&lr=&id=I9-NlkBGQjYC&oi=fnd&pg=PR5&dq=privacy+impact+assessment&ots=WH_eGUjfay&sig=EwA3UOez0KGxTresGsizHoLHLTQ&redir_esc=y#v=onepage&q=privacy%20impact%20assessment&f=true [Hämtad 9 april 2021]