LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Systemutvecklarens förhållande till digital integritet efter GDPR

En studie om hur integritet behandlas i systemutvecklingen

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Jonathan Eek
Folke Lindell
Erik Olsson

Handledare: Benjamin Weaver

Rättande lärare: Paul Pierce
Magnus Wärja

Systemutvecklarens förhållande till digital integritet efter GDPR: En studie om hur integritet behandlas i systemutvecklingen

ENGELSK TITEL: The system developers' relation to privacy post GDPR: A thesis on how privacy is handled in systems development

FÖRFATTARE: Jonathan Eek, Folke Lindell och Erik Olsson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Odd Steen, Docent, Fil Dr

FRAMLAGD: maj, 2019

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 85

NYCKELORD: Digital integritet, Integritet, GDPR, Privacy, SDLC, Systemutvecklare

SAMMANFATTNING (MAX. 200 ORD):
När GDPR trädde i kraft i maj 2018 fördes också privacyfrågan upp på agendan. Bland forskare och akademiker har ämnet digital integritet fått mycket uppmärksamhet under förhållandevis lång tid, med ramverk som Fair Information Practice Principles (FIPPs) och Privacy by Design (PbD) samt diverse riktlinjer för hur dessa ska appliceras i verkligheten. Syftet med denna uppsats är att studera hur utvecklare arbetar med digital integritet med PbD som utgångspunkt och använda GDPR som en katalysator som har aktualiserat ämnet. Vår empiri består av intervjuer med utvecklare på IT-konsultbolag för att försöka utreda hur de jobbar med digital integritet i systemutvecklingsprocessen, och hur det ser ut efter GDPR. Resultatet av vår studie indikerar att systemutvecklare har viss medvetenhet kring digital integritet, men i nuläget behandlas den ej med prioritet. Vårt resultat pekar också på att de har både kompetensen och tekniken för att kunna höja prioriteten till de nivåer som litteraturen förespråkar. Ett hinder i dagsläget är att kunderna har det sista ordet när det kommer till nivå av integritet, eftersom ägandet av koden och ansvaret i slutändan hamnar hos dem.

Innehåll

Figurer

Tabeller

1 Introduktion

1.1 Bakgrund

År 2018 var 64% av svenskarna oroliga över den ökade insamlingen och användandet av personlig digital information i samhället, vilket var 10 procentenheter mer än föregående år (Insight Intelligence, 2018). Samtidigt var dubbelt så många (40 %) jämfört med 2015 (20%) oroliga över att personlig information som de delar med sig av digitalt används i syften man inte är bekväm med (Insight Intelligence, 2018).

I sin bok Code 2.0 (2006), som diskuterar reglering av internet, skriver professor Lawrence Lessig:
"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, 2006, 79)

Även om Lessig menar att det är de som skriver koden som sätter lagarna har det kommit ett antal direktiv och lagar som försöker reglera internet och skydda privatpersoners integritet. Den senaste i raden är Dataskyddsförordningen, mer känd som GDPR (General Data Protection Regulation, (EU) 2016/679). GDPR utformades och antogs som ett skydd för individer och deras personuppgifter eftersom det är en grundläggande rättighet enligt EU:s stadga om de grundläggande rättigheterna ((EU) 2016/679, skäl 1).

GDPR var mycket omtalad under perioden innan den trädde i kraft, mycket på grund av dess omfattande natur och starka skydd för den enskilde individen, något som oroade många företag (Lindström, 2018). Arbetet med att säkerställa efterlevnad av förordningens alla artiklar ställer krav på många företag eftersom personuppgifter ofta hanteras i flera olika delar av verksamheten, exempelvis HR-system, CRM-system eller kunddatabaser. En förutsättning för att kunna efterleva kraven på ett rimligt vis är att systemen man använder är designade för att stödja detta.

En av de första gångerna man började undersöka integritet ur ett designperspektiv var i en gemensam artikel mellan Holländska och Kanadensiska dataskyddsmyndigheter 1995 (Van Rest, Boonstra, Everts, van Rijn & Paassen, 2012). Artikeln tar upp olika teknologier och komponenter som kunde höja integritetsfaktorn i system (Information and Privacy Commissioner/Ontario Canada & Registratiekamer The Netherlands, 1995). För att undvika att utvecklare skulle lösa alla integritetsproblem genom att bara addera dessa komponenter på redan existerande system vidareutvecklade en av projektdeltagarna, Ann Cavoukian, konceptet genom att introducera Privacy by Design (PbD) och dess sju fundamentala principer (Danezis, Domingo-Ferrer, Hansen, Hoepman, Metayer, Tirtea & Schiffner, 2015, Cavoukian, 2011). Tanken är att PbD med sina principer ska skapa ett holistiskt synsätt på digital integritet och bygga in detta från start till slut i processerna för företag och utvecklare ska kunna arbeta proaktivt och preventivt med integritet (Danezis et al., 2015).

Privacy by Design är omnämnt och diskuterat i förarbeten och tidiga utkast till GDPR och de två delar flera gemensamma begrepp när det kommer till hur man ska arbeta med inbyggd integritet i system och processer (COM (2012) 11 final, 2012, EDPS, 2018) Inbyggd integritet är något som blivit högaktuellt i och med GDPRs införande och dess krav på inbyggt dataskydd vad gäller utveckling av system ((EU) 2016/679, artikel 25).

"Inbyggt dataskydd (privacy by design) innebär att man tar hänsyn till integritetsskyddsreglerna redan när man utformar IT-system och rutiner. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas."
(Datainspektionen, 2019a)

Lagen lämnar fortfarande mycket utrymme för tolkning och trots att GDPR explicit inte kräver systemutveckling enligt just Privacy by Design finns det uppmaningar till detta. *"Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas[...]"* ((EU) 2016/679, skäl 78)

Spelreglerna har alltså förändrats, integritet och PbD har förts högst upp på agendan i samband med GDPR, men utvecklarnas tolkning av, och arbete med digital integritet är fortfarande i mångt och mycket upp till dem själva.

1.2 Problemområde

En av de problematiska aspekterna med GDPR och systemutveckling, som man kan utläsa när man läser vidare i skäl 78, är att det ofta inte är utvecklarna själva som bär skyldigheterna, de ska bara bygga bra förutsättningar för någon annan.

"[...]och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden kan fullgöra sina skyldigheter avseende dataskydd. "((EU) 2016/679, skäl 78)

Utvecklare är beredda i betydligt större utsträckning än användarna själva att offra användarnas digitala integritet för att uppnå exempelvis ökad funktionalitet i systemet, vilket enligt Hadar et al. (2018) kan innebära att användarnas önskemål och krav på digital integritet inte reflekteras i de färdigutvecklade systemen. Sheth et al. (2014) konstaterar att utvecklare anser dataanonymisering vara ett bättre verktyg för att tackla integritetsfrågor än lagar och regler för integritet. Vidare fann Hadar et al. (2018) att majoriteten av de utvecklare man hade intervjuat angående deras inställning till integritet hade en trångsynt och begränsad syn på konceptet digital integritet. Många av intervjuobjekten i studien hade en uppfattning om att konceptet integritet endast inkluderade säkerhetsfrågor såsom kryptering av lösenord och säkra brandväggar utåt. Respondenternas svar tyder enligt Hadar et al. (2018) på en betydande klyfta mellan rådande lagar och normer för digital integritet och deras syn på dessa. Enligt utvecklarna själva berodde detta bland annat på att man ser digital integritet som något teoretiskt, opraktiskt och abstrakt koncept (Hadar et al., 2018).

Enligt Hadar et al. (2018) saknas det forskning på hur digital integritet belyses i systemutvecklingsprocessen. Det är nämligen här som krav omarbetas till lösningar som kommer att påverka det färdiga systemet och dess användare i fråga om digital integritet, och frågan om hur utvecklare arbetar med just detta är fortfarande begränsad. Detta menar Hadar et al. (2018) påverkar det slutgiltiga systemet negativt i fråga om användarens digitala integritet, sedan utvecklarna har ett så pass stort inflytande över utformningen av systemet och dess funktioner (eller avsaknad därav). Som vi har visat exempel på ovan tycks det finnas en diskrepans i inställningen till digital integritet mellan akademiker och användare å ena sidan, och företag och utvecklare å den andra. Frågan är om denna diskrepans kvarstår även idag, efter GDPR har aktualiserat ämnet och introducerat hårdare och tydligare regelverk och lagar på området.

I en omfattande litteraturstudie av artiklar relaterade till integritet kunde Kurtz et al. (2018) konstatera att ingen vidare konceptuell utveckling skett av PbD sedan ramverket introducerades 1995 och de 7 principerna fastställdes 2009. Privacy by Design beskrivs som relativt vagt och ibland mer som ett visionärt och etiskt ramverk, det är upp till aktörer på marknaden att tolka hur det ska implementeras i praktiken (van Rest et al., 2012, EDPS, 2018). Målet med denna studie är att studera teoretiska underlag som finns för konceptet PbD och jämföra det med hur systemutvecklare faktiskt arbetar med digital integritet.

1.3 Forskningsfråga

Mot bakgrund av det identifierade och avgränsade problemområdet ställer vi oss följande forskningsfråga:

Hur behandlas digital integritet i systemutvecklarens arbete, efter GDPR?

1.4 Syfte

Syftet med denna uppsats är att med hjälp av vår empiri, baserad på ett antal kvalitativa djupintervjuer med systemutvecklare på olika IT-konsultbolag, undersöka hur digital integritet behandlas i systemutvecklares arbete efter GDPR trädde i kraft 2018. I det fall systemutvecklare jobbar med digital integritet är vi intresserade av på vilket sätt man gör det samt i vilka delar av systemutvecklingsprocessen. På så sätt ämnar vi bidra till den existerande forskningen på ämnet och se om slutsatserna hos de artiklar som vi har studerat fortfarande gäller ett år efter införandet av GDPR. Därmed blir det förlängda syftet att kunna bidra till förståelse kring hur och varför utvecklare jobbar med digital integritet på de sätt de gör.

1.5 Avgränsningar

Vi har valt att fokusera enbart på vissa delar av Systems Development Lifecycle (SDLC). De delar vi valt att fokusera på är kravställning/ kravinsamling, design samt kodning av systemet. Därmed avhandlar denna uppsats inte den första delen av SDLC vilket är planering, samt de senare delarna av SDLC som utgörs av installation, samt underhåll av systemet. Att studera

dessa faser i systemutvecklingsprocessen har definitivt sin plats, men vi har varit tvungna att avgränsa oss till de mest relevanta delarna för vår frågeställning. Detta för att säkerställa att omfånget på uppsatsen inte blir för stort och diffust, för att vi på så sätt ska kunna formulera en väl underbyggd analys och slutsats.

2 Litteraturgenomgång

Litteraturgenomgången är uppdelad som följer. Kapitlet inleds med en bakgrund till vår definition av begreppet digital integritet. Därefter ges en grundläggande beskrivning av de delar i GDPR som är mest centrala för forskningsfrågan, nämligen hur GDPR försöker säkerställa digital integritet i system. Sedan följer en genomgång och kritisk granskning av Privacy by Design, vilket är det ramverk vi har valt för att studera och utvärdera utvecklarnas arbete med digital integritet. Litteraturgenomgången avslutas med tidigare forskning på ämnet och forskares syn på bland annat problem och möjligheter med digital integritet i systemutvecklingsprocessen.

2.1 Begreppet digital integritet

Källorna till denna uppsats är nästan uteslutande på engelska, med några få undantag, vilket skapar problematik kring översättningen av vissa termer, varav den mest framträdande är "privacy". GDPR talar i huvudsak om rätten till skydd av personuppgifter,
"Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne." ((EU) 2016/679, skäl 1)
men benämns även som helhet som "rätten till integritet" senare i förordningen.
"[...]rätten till integritet i enlighet med denna förordning[...]" ((EU) 2016/679, artikel 85)
EU översätter även i andra fall "privacy" till "integritet", ett exempel är i Förslag till Europaparlamentets och Rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) där *"förordning om integritet och elektronisk kommunikation"* översätts till *"regulation on privacy and electronic communications"* i den engelska versionen (COM(2017) 10 final, 2017).
En av definitionerna av begreppet integritet enligt Svenska Akademiens ordbok (1933) lyder:
"c) förhållande(t) att icke vara utsatt (l. mottaglig) för obehörig påverkan l. inblandning, frihet från inblandning, självständighet, oberoende; i sht i fråga om makt l. inflytande o. d"
Svenska Akademiens ordboks definition i kombination med GDPR:s rätt till skydd av personuppgifter är det vi kommer att använda i vår studie. För att specifikt avgränsa oss till integritet i digitala sammanhang, exempelvis i system, har vi även valt att använda Intelligence Insights (2018) begrepp 'digital integritet', från deras årliga undersökning "Delade Meningar" om svenska folkets inställning till sådana frågor. Så med begreppet "digital integritet" syftar vi alltså till människors rätt till skydd av, samt makt och kontroll över sina personuppgifter i digitala sammanhang.

2.2 Dataskyddsförordningen (GDPR)

Dataskyddsförordningen, på engelska General Data Protection Regulation (GDPR), är en förordning som ämnar att skapa en enhetlig nivå av skydd för personuppgifter över hela Europa (Datainspektionen, 2019b). Förordningen trädde i kraft 25 maj 2018 och ersatte då det gamla dataskyddsdirektivet (direktiv 95/46/EG) och följaktligen personuppgiftslagen (PUL) vilket var den svenska implementationen av direktivet ((EU) 2016/679, artikel 94, artikel 99).

2.2.1 Laglig behandling

Enligt Artikel 5 i GDPR finns det 6 huvudprinciper för behandling av personuppgifter och kort beskrivet lyder de:

- **Laglighet, korrekthet och öppenhet**
  Att uppgifter ska behandlas lagligt, korrekt och öppet i förhållande till den registrerade ((EU) 2016/679, artikel 5.1a).

- **Ändamålsbegränsning**
  Uppgifter som samlas in får bara samlas in och användas till uttryckligt angivna berättigade ändamål ((EU) 2016/679, artikel 5.1b).

- **Uppgiftsminimering**
  De uppgifter som samlas in ska vara begränsade till den omfattning som behövs för att uppfylla ovan nämnda ändamål ((EU) 2016/679, artikel 5.1c).

- **Korrekthet**
  Uppgifter ska vara uppdaterade och korrekta i förhållande till de ändamåls de behandlas för, om inte ska de raderas ((EU) 2016/679, artikel 5.1d).

- **Lagringsminimering**
  Uppgifter ska inte lagras längre än nödvändigt för att uppfylla sina ändamål ((EU) 2016/679, artikel 5.1e).

- **Integritet och konfidentialitet**
  Uppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet med användning av lämpliga tekniska eller organisatoriska åtgärder ((EU) 2016/679, artikel 5.1f).

För behandling av personuppgifter ska alltså dessa principer efterlevas och den personuppgiftsansvarige ska även kunna påvisa detta enligt Artikel 5.2 ((EU) 2016/679).

2.2.2 Inbyggt dataskydd och dataskydd som standard

Enligt artikel 25 i Dataskyddsförordningen ska företag som behandlar personuppgifter skyldiga att genomföra lämpliga tekniska åtgärder för att garantera att endast personuppgifter som är ändamålsenliga och nödvändiga för behandlingen behandlas. Skyldigheten täcker hur mycket personuppgifter som får samlas in, tiden som det insamlade får lagras. I första hand ska åtgärderna se till att personuppgifter utan den berörda personens delaktighet görs öppen för allmänheten och att den registrerades rättigheter skyddas ((EU) 2016/679, artikel 25).

2.2.3 Säkerhet i samband med behandlingen

Artikel 32.1 i GDPR säger att personuppgiftsansvarige och personuppgiftsbiträdet ska *"vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken"* ((EU) 2016/679, artikel 32.1). Tekniker som ska användas när det är lämpligt är exempelvis kryptering och pseudonymisering. Man ska även fortlöpande kunna säkerställa att konfidentialitet, integritet, tillgänglighet och motståndskraft i de system och tjänster som används ((EU) 2016/679, artikel 32.1 b).

2.3 Privacy by Design

De senaste 30 åren har nya information- och kommunikationssystem blivit utrustade med funktioner som enklare kan samla in och övervaka privat data (Davies, 2010). Detta har gjort att forskare och beslutsfattare har blivit mer fokuserade på framväxande hot mot den digitala integriteten (Davies, 2010). På grund utav det ökade intresset och värdet på information har behovet att hantera det på ett ansvarsfullt sätt ökat drastiskt. Enligt Ann Cavoukian (2011) bör digital integritet hanteras på ett holistiskt sätt och måste bli en integrerad del av organisationens prioriteringar, planeringar, projekt och designprocesser.

"Privacy must be embedded into every standard, protocol and process that touches our lives." (Cavoukian, 2011, s. 1)

Detta ledde henne till att ta fram ett universellt ramverk, kallat Privacy by Design (PbD), för att arbeta mot det starkaste integritetsskydd som finns tillgängligt (Cavoukian, 2011). De senaste åren har intresset för PbD hos myndigheter ökat för att det hjälper organisationer att bygga in integritet i kärnan av deras tjänster och produkter från planeringsstadiet och framåt (Davies, 2010). Hadar et al. (2018) framhäver hur ramverk som PbD kan utgöra potentiella medel för att överbrygga gapet mellan utvecklarna av dessa system och lagstiftare.

2.3.1 De sju grundläggande principerna

Proactive not Reactive; Preventative not Remedial
Den första principen för Privacy by Design (PbD) handlar om att arbeta proaktivt istället för att i efterhand reagera på händelser som inkräktar på integriteten hos exempelvis användare. Privacy by Design handlar inte om att skapa åtgärder för sådana händelser, snarare att förebygga att de inte ska förekomma från första början. Cavoukian (2011) menar att för att kunna arbeta proaktivt med integritet krävs det ett tydligt åtagande för att hålla höga standarder av integritet, ofta högre än gällande lagar. Sådant arbete med integritet ska komma från den högsta ledningen och förmedlas ut till användare och intressenter för att skapa en kultur som reflekterar detta. Vidare ska det finnas etablerade metoder för att fånga upp dåliga designer eller förfaranden när det kommer till integritetsfrågor. Detta är för att på ett proaktivt och systematiskt sätt kunna identifiera och rätta till problem innan de uppstår (Cavoukian, 2011).

Privacy as the Default
Den andra principen handlar om att standarden alltid ska vara ett maximalt integritetsskydd. En användare ska inte behöva göra något för att försäkras om att deras integritet är skyddad utan det ska vara standarden, inbyggt i systemen och förvalt automatiskt.

Cavoukian (2011) presenterar ett antal så kallade "Fair Information Practices" (FIPs) som beskriver vad som ska gälla för att uppfylla "Privacy by Default":

- **Purpose Specification**
  Det ska finnas tydliga syften för insamling, användning och lagring av personliga data, de ska vara begränsade, tydliga och relevanta för omständigheterna. Dessa syften ska dessutom vara kommunicerade till användaren senast vid insamlingstillfället (Cavoukian, 2011).

- **Collection Limitation**
  Insamlingen av uppgifter ska vara rättvis, laglig samt begränsad till data som är nödvändig för att uppfylla tidigare nämnda syften (Cavoukian, 2011).

- **Data minimization**
  Förutom att man ska begränsa insamlingen av persondata till sådan som används för att uppfylla syftet, ska datan även begränsas till ett minimum av vad som behövs för att systemet ska kunna fylla sin funktion. Där det är möjligt ska kopplingen mellan data och personlig information minimeras, så att man till exempel inte kan identifiera transaktioner och interaktioner till personer om det inte är nödvändigt (Cavoukian, 2011).

- **Use, Retention, and Disclosure Limitation**
  Persondata ska inte användas till annat än de syften som är informerade till, och godkända av användaren eller av en laglig anledning. Data ska heller inte lagras längre än nödvändigt för att uppfylla uttryckta syften utan ska förstöras när syftet med datan är uppfyllt (Cavoukian, 2011).

Privacy Embedded into Design
En av de centrala delarna i PbD är att man ska arbeta med integritet i design av system och affärsprocesser på ett holistiskt, integrerat sätt, det är inget som ska komma som ett tillägg i efterhand (Cavoukian, 2011). Personlig integritet ska finnas som en grundkomponent i funktionaliteten. Cavoukian (2011) presenterar tre faktorer som ska driva arbetet mot detta mål; Man ska angripa integritetsfrågor systematiskt enligt standarder och ramverk som står upp mot externa utvärderingar i alla steg av designprocessen. Man ska utföra detaljerade riskutvärderingar när det finns möjlighet, dokumentera och publicera identifierade risker samt vilka åtgärder som tagits för att undvika dem. Den sista faktorn är att system eller teknologier ska ha en minimerad påverkan på integritet samt att användning eller felkonfiguration av systemen inte enkelt ska kunna öka denna (Cavoukian, 2011).

Full Functionality – Positive-Sum, not Zero-Sum
Cavoukian (2011) skriver att PbD har som mål att tillgodose alla intressen så att det blir en "win-win" situation, man inte ska behöva kompromissa på funktionalitet för att uppnå en hög faktor av integritet. PbD motsätter sig mot att integritet skulle konkurrera mot andra legitima intressen som till exempel design eller tekniska möjligheter utan förespråkar istället kreativitet och innovation för att uppnå full funktionalitet tillsammans med hög integritet.

End-to-End Security – Life cycle Protection
Datasäkerhet beskrivs i Cavoukians Privacy by Design från 2011 som väsentligt för att uppnå digital integritet, detta gäller hela livscykeln för all data, från det att den samlas in tills det att den förstörs efter uppfyllt syfte. Alla entiteter som behandlar data ska genom hela datans

livscykel ansvara för datasäkerheten enligt allmänt vedertagna standarder, proportionerligt mot känsligheten av datan. Vidare nämner Cavoukian (2011) metoder för att uppnå detta är säker borttagning av data, kryptering av data, accesskontroll och loggning.

Visibility and Transparency
För att få förtroende påpekar Cavoukian (2011) att det krävs transparens och insyn i de processer och de teknologier som används samt att det ska vara verifierbart av alla intressenter. För att uppnå detta vill Cavoukian att alla integritetsrelaterade policys och processer ska dokumenteras och vara tillgängliga samt att det ska finnas individer som ansvarar för dessa. Det ska finnas mekanismer för att se till att dessa policys övervakas, utvärderas och efterföljs. Det ska även finnas mekanismer för att lämna klagomål och att få upprättelse som är kommunicerade till användare (Cavoukian, 2011).

Respect for User Privacy
Den sista principen i PbD handlar om att användaren alltid ska vara i fokus. För att få bästa resultat från PbD menar Cavoukian (2011) att alla val ska vara med användarnas intressen och behov i åtanke, eftersom det är deras personliga data som hanteras. Ett av de mest effektiva sätten att undvika missbruk och felanvändning av persondata är att man ger makt till användaren. Cavoukian menar att denna makten ska ligga i samtycke, korrekt data och tillgång till den insamlade och lagrade datan. Användare ska alltid ha makt till att dra tillbaka samtycke till att deras data används, förutsatt att den används i ett syfte inte annars är tillåtet enligt lag. Användare ska ha tillgång till sin data, vara informerade om hur den används och det ska finnas mekanismer för att ifrågasätta dessa syften eller korrektheten av datan. Förutom detta nämner Cavoukian (2011) även att det måste finnas användarvänliga gränssnitt för att kunna försäkra sig om att användaren verkligen blir korrekt informerad och vet vad som händer.

2.3.2 Vagheten i Privacy by Design

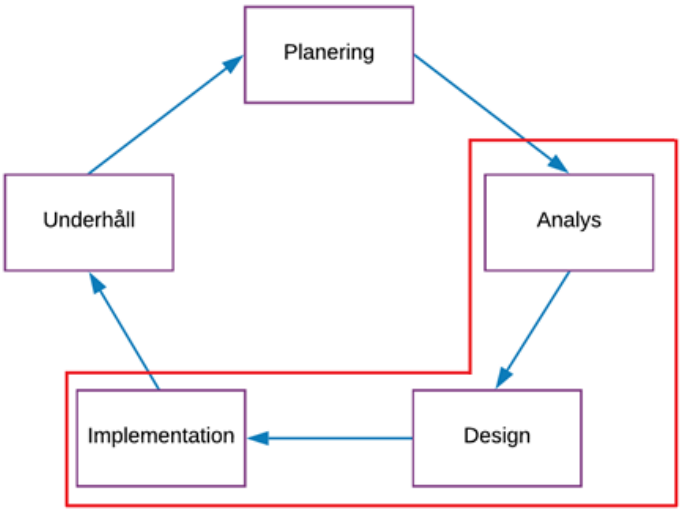
Van Rest et al beskriver i sin artikel “Designing Privacy-by-Design” (2012) PbD som ett vagt koncept som inte riktigt förklarar hur det skall implementeras i praktiken. De menar att det är mer eller mindre fritt fram för utvecklare att lägga fram en process och påstå den följer Privacy by Design. Även Chen och Williams (2013) hävdar att det saknas metodologier för hur man ska implementera PbDs principer i systemutvecklingsprocessen och själva informationssystemen. Gürses et al. (2011) kritiserar PbD för att vara luddigt och otydligt, bland annat på grund av rekursiva formuleringar som säger att PbD innebär att applicera PbD på systemutvecklingen. De konstaterar att det behövs tydligare riktlinjer och vägledning för hur systemutvecklare kan och bör arbeta med att applicera PbD rent konkret (Gürses et al., 2011).

Gemensamt för van Rest et al. (2012), Chen och Williams (2013) och Gürses et al. (2011) är att samtliga presenterar sina egna metoder för hur praktiker bör hantera PbD. Van Rest et al. (2012) beskriver hur man kan använda designmönster för att applicera PbD samt presenterar en idé till ett verktyg för hur man skall välja vilka mönsterlösningar man skall använda. Chen och Williams (2013) studerar de konceptuella grunderna för var och en av de Sju Principerna och tar fram grundläggande krav på digital integritet för informationssystem samt vid implementationen av dessa. Tanken är att detta uppstrukturerade ramverk ska hjälpa utvecklare att applicera Privacy by Design mer konkret på systemutvecklingen (Chen och Williams, 2013). Gürses et al. (2011) lyfter fram dataminimering som den mest centrala aspekten av de Sju Principerna och menar att den genomsyrar mer eller mindre alla de andra

punkterna och hela tankesättet bakom PbD. Gürses et al. (2011) menar att det behövs generaliserbara metoder som bygger på principen om dataminimering samt avråder från att använda PbD i sin grundform som en checklista för att säkra digital integritet. Istället förespråkar Gürses et al. (2011) tydliga företagspolicys för digital integritet i systemutveckling samt dedikerade experter, med kunskaper inom både juridik och systemutveckling, för att råda bot på problemet. Genom att också utbilda systemutvecklare i de sociala, ekonomiska och politiska aspekterna av digital integritet så skapas en tydligare kontext för varför det är viktigt samt bättre förståelse för hur det kan uppnås (Gürses et al., 2011).

2.4 Integritet i systemutvecklingsprocessen

Många organisationer använder sig av standardiserade systemutvecklingsmetodologier för att utveckla och stödja sina informationssystem (IS) (George & Valacich, 2016). Systemutvecklingsmetodologi är en standardiserad process som används för att följa alla de kritiska stegen för att planera, analysera, designa, implementera och underhålla sina IS (George & Valacich, 2016). De tre faser vi har avgränsat oss till är Analys, Design och Implementation.



Figur 1: Systems Development Life Cycle med George & Valacich (2016) faser och vår avgränsning.

Många processer följer samma mönster och livscykel, som till exempel att en produkt utvecklas, testas, släpps på marknaden, säljs, till den till slut ersätts av en annan produkt (George & Valacich, 2016). Systems development lifecycle (SDLC) är en vanlig metodologi för systemutveckling inom många organisationer (George & Valacich, 2016). SDLC delar upp projektet i faser för att få en överblick över utvecklingen av projektet (George & Valacich, 2016). SDLC finns i olika utförande där allt från 3 till 20 faser kan beskrivas (George & Valacich, 2016). En processmodell täcker alla relevanta faser i systemets livscykel som underlättar ägaren att följa projektets resultat, tidsåtgång och kostnader (J. van Rest et al., 2012). För att stödja Privacy by Design genom systemutvecklingsprocessen behövs olika medel. Hoepman (2014) menar att det under systemutvecklingsprocessen finns ett antal praktiska metoder du kan använda för att säkerställa användarens digitala integritet, men att dessa är koncentrerade till implementationsfasen. Dock finns det väldigt lite konkret

integritetsfrämjande stöd att tillgå i början av processen och utvecklaren eller arkitekten står därför mer eller mindre tomhänt under designfasen (Hoepman, 2014). Detta beror till stor del på att designmönster är mer inriktade mot specifika tekniska problem under kodning och implementation (Hoepman (2014). Samtidigt understryker Kallionatis et al. (2008) vikten av att hantera frågor om digital integritet i designfasen snarare än under implementeringen av systemet.

2.4.1 Förkrav på integritet

Enligt Datatilsynet (2017) och Microsoft (2012) är förståelse för dataskydd och informationssäkerhet en nödvändig förutsättning för att utveckla mjukvara med ett integritetstänk innan projektet startar. Anställda borde veta vilka krav som gäller och vad de ska tänka på när de utvecklar system med dataskydd. De bör också ha förståelse för vilken metodologi och vilka rutiner som ska följas. Organisationen bör därför införa utbildningar om integritet och hur det ska inkorporeras i systemutvecklingsprocessen, samt införa policys (Cavoukian, 2011, Cavoukian, Taylor & Abrams, 2010). De uppmanas också att använda en etablerad utvecklingsmetodologi som reflekterar ett integritetstänk och se till att den efterföljs (Datatilsynet, 2017). Cavoukian et al. (2010) trycker på att tidig vägledning i integritetsarbetet skapar ett stort mervärde för organisationen. Fångas de tidigt, kan integritetsfallgropar undvikas och integritetstänket inbäddas i designen av systemen. Dessa åtgärder är då så kallade proaktiva aktiviteter för att förebygga intrång på användares integritet och hålla en hög integritetsstandard på systemet (Cavoukian, 2011). Dessa aktiviteter kallar Microsoft (2012) för en slags förkrav innan utvecklingsprocessen sätts igång.

2.4.2 Analysfasen

George & Valacich (2016) beskriver att i den andra fasen, analys/undersökningsfasen, studeras organisationen processer och nuvarande informationssystem som används i verksamheten noggrant. Denna fas är uppdelad i två delar. Den första delen handlar om att granska verksamhetens processer och befintliga system. Genom observationer av processerna och intervjuer med användarna identifieras kraven som användarna vill ha från det tänkta systemet. George & Valacich (2016) fortsätter att i den andra delen formuleras, struktureras och utvärderas kraven för att ta bort överlappningar och redundans. Arbetet under analysfasen leder till en systembeskrivning av ett potentiellt system som skulle kunna användas. Denna beskrivning kan sedan användas som en rekommenderad lösning för det kommande systemet.

För att inkorporera integritet i denna fasen skriver Datatilsynet (2017) och Cavoukian (2011) att man måste definiera exakt vad för typ av data som ska samlas in och vad den ska användas till. När krav på integritet, säkerhet och säkerhetsrisker upptäcks tidigt, kommer utvecklarna veta vilka krav de behöver möta och det kan öka informationssäkerheten och dataskyddet under hela systemutvecklingsprocessen (Datatilsynet, 2017). Säkerhetskraven för systemet bestäms genom att identifiera vilka risker systemet kan utsättas för och vilken risk företaget är villig att ta. Detta definierar vilka relevanta parametrar som systemet ska använda (Datatilsynet, 2017). J. van Rest et al. (2012) beskriver att intergritetskraven bör utgöra en väsentlig del av systemkraven. Det som tagits upp i systemkraven kan leda till en bättre design där dessa krav har beaktats. För att få en lättare översikt och kunna följa kraven som ställs genom SDLC, kan man med fördel utforma en checklista (Datatilsynet, 2017). Kravställning och designfasen är, enligt Hoepman (2014), centrala eftersom det framförallt är

beslut i dessa faser som bestämmer hur väl det slutgiltiga systemet värnar om användarens digitala integritet.

2.4.3 Designfasen

Den tredje fasen av SDLC är design. Under designfasen översätts den rekommenderade lösningsbeskrivning till en logisk designspecifikation sedan en fysisk designspecifikation (George & Valacich, 2016). I den logiska systemspecifikation designas främst den affärsmässiga aspekten av systemet, alltså den del av systemet som användaren interagerar med i det dagliga arbetet (George & Valacich, 2016). Allt från data för inmatning och utmatning till databaser, processer, och rapporter. Här är det viktigt att se till att integritetskraven från systembeskrivningen kommer med, som att mängden och omfattningen av data som samlas in matchar behovet (Datatilsynet, 2017). Den logiska specifikationen är oberoende av någon specifik hård- och mjukvara, utan är till för att skapa en idé över det tänkta systemets funktioner (George & Valacich, 2016). Cavoukian (2011) menar att det är extra viktigt att angripa integritetsfrågorna på ett systematiskt sätt i designfasen, vilket kan göras med hjälp av ramverk och standarder. Utöver det ska man utföra riskutvärderingar där det är möjligt. Risker som upptäcks ska dokumenteras, publiceras tillsammans med stegen som vidtagits för att undvika dem (Microsoft, 2012, Datatilsynet, 2017, Cavoukian, 2011).

2.4.4 Implementationsfasen

Den fjärde fasen i SDLC är implementation. Implementationen innehåller kodning, testning och installation. Kodningen sköts av programmerare som bygger systemet (George & Valacich, 2016). Säker kodning bör fram främjas. Gärna genom att skapa en lista med tydligt definierade verktyg och kodbibliotek som är godkända (Datatilsynet, 2017). Att tidigt investera tid och ansträngning i effektiva praxis hjälper till att eliminera säkerhetsrisker och minskar risken behöva åtgärda dem senare i processen eller efter implementationen (Microsoft, 2012). Att hitta och åtgärda problem efter implementationen av ett system är mycket dyrare än att åtgärda det i ett tidigt stadie (George & Valacich, 2016). Danezis et al. (2015) förespråkar att en integritetspolicy upprättas som ser till att systemet upprätthåller en viss standard av integritet. Åtminstone ska den vara kompatibel gällande de legala krav som ställs. Sedan är det viktigt att se till att policyn efterlevs. Detta faciliterar och automatiserar säkerhetsproceduren för säker kodning (Datatilsynet, 2017). Koden ska löpande under utvecklingens gång granskas och analyseras så att den följer de riktlinjer som satts (Datatilsynet, 2017).

Under testfasen testas delar av eller hela systemet för att hitta och rätta till buggar som uppstått (George & Valacich, 2016, Datatilsynet, 2017). Tester ska göras för att säkerställa att kraven på dataskydd och säkerhet från designen och kodningen är uppfyllda och implementerade i systemet (Datatilsynet, 2017). Checklistan som tagits fram i kravställningen kan användas som underlag för att lättare kunna se till att allt gjorts Datatilsynet (2017). Slutligen, när installationen börjar, implementeras det nya systemet in i det dagliga arbetet, med upplärning support och dokumentation. (George & Valacich, 2016)

2.5 Utvecklares syn på digital integritet

2.5.1 Innan GDPR

I en artikel publicerad i april 2017 redogör Hadar et al. för sin kvalitativa intervjustudie av mjukvaruutvecklares inställning till integritet. En av artikelns huvudteser är att utvecklarna, i en era som ännu inte berörts av GDPR:s lagstadgade krav på digital integritet, besitter stor makt över i vilken utsträckning de system man utvecklar är i framtagna i enlighet med PbD eller ej. Därmed blir deras uppfattning om, och inställning till, konceptet digital integritet, av stor vikt för det slutgiltiga systemet (Hadar et al., 2018). Författarna menar efter en grundlig litteraturgenomgång att det finns stort behov av forskning på området men konstaterar samtidigt att det inte har hänt särskilt mycket på området på flera år. De påpekar samtidigt att de efter sin litteraturstudie fortfarande är osäkra på hur effektiva ramverk som PbD är på att överbrygga gapet mellan utvecklare och lagstiftare, samt vilka eventuella tillkortakommanden PbD har i praktiken.

2.5.2 Teori och praktik

Birnhack et al. (2014) fann stora klyftor mellan lagen och tekniken den försöker reglera då vedertagen litteratur om dataskydd i IT-system förespråkar behandling av data som i vissa fall går emot PbD. De nämner vad som då fortfarande bara var planer på att lagstadga kring PbD i GDPR, och konstaterar att något drastiskt måste göras för att minska gapet mellan teori och praktik, lag och teknik. (Birnhack et al., 2014) Enligt Gürses et al. (2011) är den inbyggda vagheten i PbD symptomatisk för avståndet mellan beslutsfattare och systemutvecklare i förståelsen om hur man rent tekniskt ska implementera dataskydd. Tack vare att PbD tar sig olika uttryck i olika policydokument möjliggörs tolkningen att det gäller insamling av vilken data som helst som man helt enkelt bara sätter en stämpel för digital integritet på.

En av slutsatserna i Hadar et al. (2018) är att uppfattningen av och inställningen till digital integritet hos många av de intervjuade utvecklarna skiljer sig markant från rådande normer och ramverk som föreskrivs av forskare. Majoriteten av utvecklarna i studien har svårt att skilja på koncepten informationssäkerhet och integritet vilket ger upphov till att många av dem arbetar allt för snävt med PbD i sitt dagliga arbete, och bara inkluderar ett fåtal av de sju principerna i PbD. Ingen av de 27 intervjuade utvecklarna hade ifrågasatt ett systems fundamentala arkitektur i fråga om inbyggd digital integritet eller kunde beskriva situationer där de ändrat arkitekturen för att stödja och förbättra digital integritet i slutprodukten. (Hadar et al., 2018)

2.5.3 Ansvarsfördelning och synen på digital integritet

Vidare tycks affärsmässiga behov och företagets intressen prioriteras högre av utvecklarna än att värna om slutanvändarens digitala integritet. Flera respondenter berättar att de inte implementerar funktionalitet för digital integritet eftersom det är orealistiskt i många system. (Hadar et al., 2018) Samma trend reflekteras i organisationen i stort; 17 av 27 utvecklare beskriver policys och normer i företaget som inte är i enlighet med PbD alternativt helt saknar någon policy för arbete med digital integritet. Följden blir att dessa utvecklare inte arbetar enligt PbD, antingen för att de aktivt uppmuntras att inte göra det eller inte tänker på sådana frågor överhuvudtaget eftersom det inte existerar på företagets radar.

Vissa utvecklare i praktiken är villiga att offra användarens integritet till fördel för utökad funktionalitet i systemet. Hadar et al. (2018) påpekar att en högre grad av inbyggd integritet i systemet också kan utgöra hinder för användaren genom exempelvis minskad personalisering. Detta är alltså en avvägning som utvecklarna måste ta ställning till under systemutvecklingsprocessen.

Hadar et al. (2018) kunde också identifiera en tydlig tendens bland utvecklare att inte ta ansvar för frågor om digital integritet i systemutvecklingsprocessen, utan uppgav istället att detta ansvar ligger på någon annan. Samtidigt beskriver en utvecklare hur företaget hade implementerat en ny policy efter att ha blivit stämda av en kund. Stämningen berodde på att kunden upplevde att deras personuppgifter hade misskötts, varpå företaget ändrade sina rutiner, trots att det inte fanns några lagkrav på att göra det utan endast för att skydda sina egna intressen framöver (Hadar et al., 2018). Slutligen konstaterar författarna att frågan om digital integritet ses som ett socialt problem snarare än ett tekniskt eller juridiskt problem, vilket också stämmer väl överens med resultaten i studien av Birnhack et al. (2014).

2.6 Litteratursammanfattning

Från teorin kan vi härleda ett antal faktorer som är återkommande när det kommer till hanteringen av integritetsfrågor inom systemutveckling.

Synen på begreppet digital integritet eller privacy
Hadar et al. (2018) menar att hur verksamhet och utvecklare tänker kring integritetsfrågor har en tydlig påverkan på hur de arbetar med det. Förutom det så är det väldigt många utvecklare som blandar ihop integritet med datasäkerhet, vilket gör att integritetsperspektivet glöms bort (Hadar et al., 2018).

Utbildning
Kopplat till synen på digital integritet kommer utbildning inom ämnet, både Microsoft (2012) och Datatilsynet (2017) menar att förståelse för exempelvis dataskydd och informationssäkerhet är en nödvändig förutsättning för att kunna utveckla mjukvara med integritetstänk.

Interna policys angående digital integritet
Hadar et al. (2018) menar att organisationer som saknar policys och normer för hur de ska arbeta kring integritet reflekteras även i praktiken hur deras utvecklare arbetar. Cavoukian (2011) har ett fokus på policys i flera av sina principer, för att kunna arbeta proaktivt, öppet och transparent.

Utvärderingar av risker
Cavoukian (2011) rekommenderar detaljerade riskutvärderingar där det finns möjligheter vilken även stödjs i både Microsofts (2012) och Datatilsynets (2017) mer praktiska tillämpningar av integritet och säkerhet. Även GDPR utgår till stora delar utifrån vilka risker som finns när olika nivåer av skydd ska tillämpas.

Datasäkerhet och dåliga designer
Cavoukian benämner datasäkerhet som väsentligt för att uppnå en hög grad av integritet, att data skyddas under hela dess livscykel. GDPR har krav på att det ska säkerställas en

säkerhetsnivå som är "lämplig i förhållande till risken" samt både Microsoft (2012) och Datatilsynet (2017) framhäver säkerheten som krav på systemen. Dåliga designer ska systematiskt kunna upptäckas och den koden som skrivs ska löpande granskas (Cavoukian, 2011, Datatilsynet, 2017).

Påverkan i systemutvecklingsprocessens olika delar

En central del med integritetsarbetet är att man ska arbeta holistiskt med det (Cavoukian, 2011). Alla delar i processen har någon påverkan eller aktivitet, dels måste man se till att rätt krav blir ställda på systemet och sedan att de faktiskt blir implementerade.

Slutanvändares rättigheter

GDPR ställer samma krav som Cavoukian (2011) tar upp i principen om Privacy as the Default: För att samla in data om en person krävs det tydliga, begränsade och relevanta syften för insamlingen. Data får inte användas till annat än de syftena och ska vara i samtycke med användaren eller enligt annan laglig anledning. Insamlingen ska vara begränsad till den data som är nödvändig för att uppfylla syftet och ska inte lagras längre än nödvändigt (Cavoukian, 2011, GDPR).

Förutom detta ska även användaren ha möjlighet till insyn och tillgång till den insamlade datan samt möjlighet att dra tillbaka samtycket (Cavoukian, 2011, GDPR).

Tabell 1: Litteratursammanfattning

Kategori	Undersökningsområden	Litteratur
Synen på begreppet digital integritet eller privacy	• Utvecklare tenderar att blanda ihop digital integritet med säkerhet • Ordets betydelse för personen • Positive-Sum not zero-sum	Hadar et al. (2018), Birnhack et al. (2014), Cavoukian (2011)
Utbildning	• Proaktivitet • Förkunskap • Förståelse	Datatilsynet (2017), Microsoft (2012), Cavoukian (2011) Gürses et al. (2011)
Interna policys	• Tydligt åtagande från organisationen • Transparens • Normer och ansvar Reflekteras i praktiken	Cavoukian (2011), Hadar et al. (2018), Gürses et al. (2011), Danezis et al. (2015), Cavoukian, Taylor, Abrams (2010)
Utvärderingar av risker	• Systematiskt arbete • Säkerhet i förhållande till risker	Datatilsynet (2017), Microsoft (2012), Cavoukian (2011), GDPR Chen & Williams (2013)
Datasäkerhet och dåliga designer	• End-to-end security • Lämpliga åtgärder som anoymisering, pseudonymisering, kryptering • Kvalitet	Cavoukian (2011), Microsoft (2012), Datatilsynet (2017), GDPR Hadar et al. (2018) Hoepman (2014), Cavoukian et al. (2010)
Påverkan i systemutvecklings-processens olika delar	• Holistiskt synsätt • Kravställning • Analys • Design • Implementation	George & Valacich (2016), George & Valacich (2016), Datatilsynet (2017), Microsoft (2012), Cavoukian (2011), Hadar et al. (2018), Hoepman (2014), Kalloniatis et al. (2008)
Slutanvändares rättigheter	• Purpose limitation • Collection limitation • Data minimization • Use, Retention, and Disclosure Limitation	Cavoukian (2011), GDPR Gürses et al. (2011)

3 Metod

3.1 Metodval

Efter att ha formulerat någon slags hypotes om ämnet och hur det skulle kunna se ut i verkligheten vände vi oss till tidigare forskning för att utvärdera hypotesen och skaffa oss en uppfattning om hur det har sett ut tidigare, vilken relaterad forskning som har utförts och vad den har kommit fram till. Tidigare forskning som till exempel Hadar et al. (2018), som diskuterade utvecklares syn på digital integritet, gjorde oss nyfikna på om arbetet med digital integritet kanske hade förändrats efter yttre påtryckningar som GDPR. För att undersöka detta krävdes empiri, frågan var bara i vilken form?

3.1.1 Kvalitativa studier

Eftersom målet var att undersöka hur utvecklare arbetar med digital integritet och hur deras arbetssätt påverkas av integritetskrav valde vi en kvalitativ ansats för datainsamlingen. Den kvalitativa metoden fokuserar på detaljer, nyanser och det unika hos intervjuobjektet genom att man låter hen framföra sina åsikter och tolkningar (Jacobsen, 2002). Detta är något som passar väl in på vår studie då integritet och PbD som vi visat ovan inte alltid är solklart och vi ville studera hur systemutvecklare arbetar med digital integritet.

En av de främsta styrkorna som Jacobsen (2002) lyfter fram med en kvalitativ studie är möjligheten att uppnå hög intern giltighet. Genom att utföra semistrukturerade intervjuer där vi t ex kan kasta om ordningen på frågorna baserat på respondentens svar, ställa spontana följdfrågor och erbjuda en öppen diskussion i slutet, så färgar vi som forskare inte respondentens svar lika mycket som om vi hade arbetat med exempelvis enkäter. Resultatet blir en högre grad av intern giltighet vilket är viktigt i vårt fall, då det innebär större sannolikhet att få fram sanningen om ett fenomen eller problem som inte är studerat i någon större utsträckning (Jacobsen, 2002). Vilket är fallet med utvecklares arbete med PbD.

Nackdelen med detta angreppssätt är att det är resurskrävande (Jacobsen, 2002). Detta var något vi märkte dels för egen del, men också eftersom vi i första hand försökte hitta personer med någon högre position. Dessa var svårare att få tag på och kanske inte hade tid att träffa oss för en längre djupintervju. Jacobsen (2002) nämner också att en svårighet kan uppstå med flexibiliteten genom att det dyker upp ny information som gör det svårt att känna att man fått med all data. Ett annat problem Jacobsen (2002) skriver om är generaliseringsproblem som kan uppstå och är en av de största nackdelarna med kvalitativa studier, vilket i sin tur gör att man måste vara försiktig med att generalisera dem för mycket (Jacobsen, 2002).
Enligt Jacobsen (2002) kan en kvantitativ metod sätta en ytlig prägel på undersökningen. Eftersom vår frågeställning krävde en djupare inblick i intervjuobjektens arbetssätt och medvetenhet hade vi potentiellt kunnat gå miste om vital information och insikter. Vilket hade kunnat göra att vår forskningsfråga inte hade kunnat besvaras med samma djup och förståelse. Vidare beskriver Jacobsen (2002) att ett alltför stort avstånd mellan undersökare och

undersökt kan skapa ett problem gällande förståelse för det som ska undersökas. Därför bestämdes det att en kvalitativ metod var att föredra till denna studie.

3.2 Datainsamling

3.2.1 Litteratursökning

För att hitta teori använde vi oss utav Google Scholar, LUBsearch och Association of Information systems eLibrary för vetenskapliga artiklar samt Google för mindre akademiska källor som Insight Intelligences 'Delade Meningar'. De sökord vi huvudsakligen använde oss utav var följande:

- GDPR
- Privacy by Design
- Privacy
- Systems Development Lifecycle
- SDLC
- Developer
- Solution Architect

Vi har även använt oss utav en mix av dessa orden när vi gjort sökningar.

3.2.2 Urval av respondenter

Innan vi kontaktade några företag började vi med att fastställa några kriterier för våra potentiella respondenter. Efter kriterierna var satta, identifierade vi ett antal företag som uppfyllde dem och började skicka ut mail och frågade om de kunde ställa upp på intervju.

Kriterierna som identifierades är:

- IT-konsult - Vår tanke var att konsulter skulle kunna representera en större bredd i erfarenheten när det kommer till olika projekt, företag och branscher. Ytterligare en anledning var hypotesen om att utvecklare som arbetar som konsulter skulle kunna tänkas prata mer öppet och frispråkigt om projekt som de deltagit i. Detta eftersom konsulter kanske inte känner samma plikt gentemot kunder som inhouse-utvecklare känner för det egna företaget.
- Erfarenhet med att arbeta med projekt som behandlat personuppgifter före och efter GDPR - För att få respondenter med ett bredare perspektiv ville vi ha personer som arbetat med personuppgiftshantering både före och efter GDPR.
- Gärna någon projektledare eller någon med en överblick över krav, design och utveckling med bakgrund som systemutvecklare. Eftersom vi undersöker flera delar av systemutvecklingsprocessen vill vi gärna intervjua någon med erfarenhet och överblick över systemutvecklingsprocessen.
- Personer från olika företag - Vi antog att på ett visst företag arbetar man utifrån samma policys och arbetssätt. Därför kom vi fram till att vi endast skulle ha ett intervjuobjekt från varje företag för att få en större spridning på arbetssättet.

Tabell 2: Respondenter

Namn	Kön, ålder	Yrkesroll/titel	Företag	Intervjutyp	Tid	Appendix
Respondent 1	Man, 30	CTO, Tech lead	IT-konsultbolag, Organisation 1	Personligt möte	39 min	A
Respondent 2	Man, 30	Mjukvaruarkitekt, systemutvecklare	IT-konsultbolag, Organisation 2	Personligt möte	44 min	B
Respondent 3	Man, 29	Integrations-specialist, systemvetare	Pulsen Integration, Organisation 3	Personligt möte	29 min	C
Respondent 4	Man, 34	Solution architect, senior software developer	IT-konsultbolag, Organisation 4	Personligt möte	49 min	D

3.2.3 Intervjuguide

Alla intervjufrågor är baserade på och förankrade i teorin, vilket gör det enklare att kritiskt granska och replikera vår studie. Samtidigt underlättar det också att ställa empirin i kontext till litteraturen, vilket är av extra stor vikt eftersom flera av källorna efterfrågar mer forskning på ämnet för att minska diskrepansen mellan teori och praktik.

Intervjuguiden har utvärderats och finslipats efter varje intervju, baserat på nyanser och nya infallsvinklar som vi fått efter de olika intervjuerna. Det faktum att man kan ändra upplägget på undersökningen efter hand som den tar form lyfter Jacobsen (2002) fram som en av styrkorna med kvalitativa studier. Detta bidrog också till att valet av empirisk undersökningsmetod föll på den semistrukturerade intervjun. Jacobsen (2002) rekommenderar en sådan typ av undersökning i situationer då ämnet inte är beforskat i någon större utsträckning, som i vårt fall.

Från ramverket som utformades utifrån litteraturen skapade vi en intervjuguide för de områden vi ville undersöka empiriskt. Eftersom vi skulle använda oss av en semistrukturerad intervju så var syftet med intervjuguiden inte att lägga upp en exakt instruktion utan mer en vägledning för vilka områden som skulle undersökas. Således har vi utgått från exempelfrågor kopplade till områdena i vårt ramverk, men det har däremot inte funnits några krav på att dessa skulle följas exakt i varken ordning eller formulering. Vid behov kunde vi under intervjuerna avvika från mallen och ställa frågor så som det passade bäst vid tillfället. Om intervjuobjektet tog upp något om till exempel kravställning så kunde vi följa upp med en fråga om det var där i processen som de tyckte att integritet hade störst vikt eller påverkan. Förutom dessa undersökningsområden så innehöll intervjuerna även allmänna diskussioner om vad intervjuobjekten ansåg hade förändrats mest, dels i deras arbete dels i

utvecklingsprocessen sedan GDPR. Nedan syns exempelfrågor, kopplade till olika områden, som formulerades utifrån ramverket som vi skapat med hjälp av litteraturen.

Tabell 3: Intervjuguide

Kategori	Undersökningsområden	Exempelfrågor
Synen på begreppet digital integritet eller privacy	• Utvecklare tenderar att blanda ihop digital integritet med säkerhet	• Vad betyder begreppet digital integritet eller privacy för dig? • Anser du att krav på digital integritet hämmar innovationen inom systemutveckling?
Utbildning	• Proaktivitet • Förkunskap • Förståelse	• Är du bekant med konceptet privacy by design? • Är du bekant med lagar som berör integritet i informationssystem (privacy)? • Har du fått någon utbildning relaterad till privacy i systemutveckling?
Interna policys	• Tydligt åtagande från organisationen • Transparens • Normer och ansvar Reflekteras i praktiken	• Har ni några interna policys, liknande dokument eller normer för hur ni ska arbeta med privacy i era projekt? Isåfall, förmedlas dessa till kunder och andra intressenter på något vis?
Utvärderingar av risker	• Systematiskt arbete • Kvalitet • Säkerhet i förhållande till risker	• Har ni några etablerade metoder för att identifiera risker eller dåliga designer när det kommer till privacy problematik? När under processen görs det i så fall den typen av riskutvärderingar?
Datasäkerhet och dåliga designer	• End-to-end security • Lämpliga åtgärder som anonymisering, pseudonymisering, kryptering • Kvalitet	• Hur arbetar ni med säkerheten för data som samlas in och lagras? • Har ni någon som någon som säkerställer koden, att den uppfyller intergritetskrav? Gör ni t.ex. code reviews?
Påverkan i systemutvecklings-processens olika delar	• Holistiskt synsätt • Kravställning • Analys • Design • Implementation	• Genomgång av vad som görs i varje del av processen • Vilken eller vilka delar av systemutvecklingsprocessen anser du påverkas mest av krav på privacy?
Slutanvändares rättigheter	• Purpose limitation • Collection limitation • Data minimization • Use, Retention, and Disclosure Limitation	• Har ni några specifika metoder eller tekniker för att hantera datas livslängd? Gör ni egna undersökningar för att kontrollera kundens syften med den data som samlas in eller förutsätter in att kunden har gjort det? • Undersöker ni själva om systemen samlar in mer data än vad som behövs för ändamålet? • Har ni arbetat något med slutanvändares rätt till sina personuppgifter; som att ta del av dem, att de ska vara “korrekta” eller att användare kan dra tillbaka samtycken?

3.2.4 Genomförande

Slutligen har vi valt att utföra alla intervjuer personligen på plats ute hos företagen. Detta eftersom människor, enligt Jacobsen (2002), har lättare för att öppna upp sig och prata om känsliga frågor när de pratar med intervjuaren ansikte mot ansikte. Anledningen är att intervjuobjektet känner sig tryggare i en sådan situation, då hen får ett ansikte på personen som ställer frågorna och på så sätt kan uppfatta subtila signaler, minspel etc. som går förlorade över telefon. Därför är det, menar Jacobsen (2002), olämpligt att använda sig av telefonintervjuer för öppna, personliga intervjuer som våra, då respondenten är mindre benägen tala sanning i en sådan situation.

3.3 Transkribering och analys

Vi valde att transkribera intervjun för att lättare kunna analysera, jämföra och bearbeta det empiriska materialet. Jacobsen (2002) påpekar att transkribering även underlättar arbetet med intervjumaterialet genom att tillåta kommentarer och understrykningar i texten på ett sätt som inte är möjligt med inspelade ljudfiler. Alla intervjuer finns transkriberade i appendix, men överensstämmer inte till hundra procent med inspelningarna. Detta beror på att vi ville öka läsbarheten genom att utelämna stakningar, upprepningar och talspråk som enbart försämrar läsbarheten och inte tillför något konkret till empirin. Transkriberingen gjordes kort efter intervjuerna för att kunna ha minnet färskt med sammanhangen de berättat saker i.

3.3.1 Kodning av transkribering

För att underlätta analys av svaren i transkriberingen, som slutade på ungefär 18 000 ord, läste vi igenom transkripten för analysera svaren och kodade de svaren utifrån litteratursammanfattningen som visas i tabell 1. Kodningen är gjord för att vi lättare ska kunna navigera i transkripten vid sammanställningen av empirin. Koderna är satta där vi anser att intervjuobjektets svar passar in på en viss kategori, ett längre svar kan ha berört flera ämnen vilket har gjort att ett svar kan ha fått flera koder. För att säkerställa att kodningen har gått rätt till har vi tillsammans diskuterat svaren och sedan satt den koden vi ansett passat in till de specifika svaren.

Tabell 3 har ytterligare en kategori jämfört med Tabell 1. Detta beror på att vi under intervjuerna och transkriberingen fann svar som vi inte hade räknat med vid sammanställningen av litteraturgenomgången, men som skulle kunna vara intressant för vår studie samt vidare forskning. Därför bestämdes också att denna kategori ska tas med i kodningen. Kategorin “Ansvarsfördelning” i Tabell 3 syftar på det faktiska respektive det självupplevda ansvaret som konsulterna har för systemen som de levererar till kund.

Tabell 4: Kodöversikt

Kod	Kategori
DI	Synen på begreppet digital integritet
U	Utbildning
IP	Interna Policys
RI	Utvärderingar av risker och dåliga designer
DS	Datasäkerhet
SP	Påverkan i systemutvecklingsprocessens olika delar
SR	Slutanvändarens rättigheter
AF	Ansvarsfördelning

3.4 Etiska aspekter

Inför intervjuerna erbjöds alla respondenter att ta del av intervjuguiden för att minska deras osäkerhet kring själva intervjun och vad den kunde tänkas innehålla. Oates (2005) framhäver att det kan vara ett bra sätt att visa att man är en seriös forskare och samtidigt ge intervjuobjekten möjlighet att reflektera över frågorna. Samtliga respondenter och deras organisationer erbjöds också möjligheten att förbli anonyma. Detta är enligt Oates (2005) en viktig aspekt för etisk forskning, inte minst för att säkerställa att det inte blir några repressalier för respondenterna pga. att de exempelvis delar med sig av känslig information. Slutligen bad vi respondenterna om tillåtelse att spela in samtalet för att lättare kunna bearbeta det i efterhand.

I samband med alla intervjuer följde vi Oates (2005) regler och rekommendationer för etisk forskning inom informationssystem. Alla respondenter fick information om vilka vi är, studiens syfte och hur vår empiri är uppbyggd samt hur och vad den ska användas till. Intervjuobjekten blev också informerade om möjligheten att dra sig ur studien, samtidigt som de fick möjlighet att läsa transkriberingen i sin helhet om de önskade, i enlighet med Oates (2005) föreskrifter. Hon understryker att dessa steg är viktiga för att öka studiens transparens och tryggheten hos intervjuobjektet och att korrekturläsning av transkriberingen säkerställer att båda parter har samma bild av intervjun och vad som sagts.

3.5 Validitet

Eftersom vår empiri är begränsad vad gäller antalet intervjuer bör detta tas i beaktande vid vidare användning av slutsatserna som den ligger till grund för. Eftersom det empiriska materialet består av fyra djupintervjuer med IT-konsulter bör resultaten endast ses som indikatorer på olika fenomen och resultat, snarare än vedertagna sanningar. Den här studien

bör ses ur en svensk kontext, och det är fullt möjligt att resultaten hade sett annorlunda ut i andra länder, med andra företag, lagar och kulturer.

4 Empiri

I kapitel fyra sammanställs resultaten av vår empiriska undersökning. Svaren från de semistrukturerade intervjuerna är kodade efter ett antal olika kategorier från vår litteratursammanfattning, och som beskrevs i kapitel tre. Detta kapitel är sedan indelat enligt samma kategorier. Transkripten återfinns i Appendix A-D.

4.1 Syn på begreppet digital integritet eller privacy

Personlig åsikt om digital integritet
Synen på vad digital integritet är för dem är relativt enstämmig bland våra respondenter. Alla menar att digital integritet är viktigt för dem. De beskriver att det handlar om att man själv bestämmer och har kännedom om vad som händer med sin personliga data, till exempel att företag kan använda datan för att hålla reda på vad man gör, genom att använda GPS-tracking eller att man loggas. De nämner även att man ska kunna "opt-out" från att företag samlar in information om dem. Två av intervjuobjekten nämner även att de aktivt själva gör val utifrån deras syn på integritet. Till exempel att använda NoScript i webbläsaren för att hindra webbsidor från att samla in information den vägen, eller väljer bort företag som de anser samlar in för mycket information, till exempel Facebook. Samt att man ibland aktivt lämnar telefonen utanför mötesrummet vid viktiga möten på grund utav att man är rädd för att telefonen spelar in det som sägs.

Endast en av respondenterna, Respondent 2 (R2), nämner uttryckligen att det är så pass viktigt att han tycker att det inte är tillräckligt många andra i samhället som tycker det är viktigt, men att GDPR är ett steg i rätt riktning. Även Respondent 3 (R3) vill att det ska finnas starkare lagar som rör digital integritet, på grund utav att misstankar om att mobilen avlyssnar samtal.

Om krav på digital integritet hämmar utvecklingen
På frågan om krav på digital integritet hämmar utvecklingen har våra respondenter lite delade meningar. Två ser inte det som ett så stort problem att det inte går att bygga runt kraven, utan menar att det är en möjlighet att skapa bättre lösningar. R2 menar att det kan ha viss inverkan på vissa system som finns just nu och måste förhålla sig till det, men om integritetstänket finns med från starten så anser han inte att det skulle vara så stort problem.

De andra två, Respondent 1 (R1) och Respondent 4 (R4), anser att det hämmar innovationen och pekar på att de fått tacka nej till uppdrag på grund utav krav som gjort att de inte kunnat genomföra uppdraget och att arbetsbördan har ökat i och med kraven. R1 säger även att han ser problem om det inte hade funnits några krav alls, men att vi hade kunnat *"röra oss i en betydligt högre hastighet om vi inte hade haft några betänkligheter kring sådana saker. Sen hade vi fått många andra problem på köpet"* (Appendix A, #54).

4.2 Utbildning

Två av fyra respondenter berättar att de har obligatoriska utbildningar om GDPR för alla utvecklare inom organisationen. Av dessa så har Organisation 1 (O1) kurser internt där R1 är den som hållit i utbildningen, som också har erbjudits till kunder. Dels genom att kunder har bjudits in till kontoret och dels att utbildningarna sålts som "white labelled" produkter, alltså att R1 hållit i utbildningar i kundens namn. I Organisation 2 (O2) så har man tagit fram en E-learning kurs som man själv läser och tentar av i en webbportal.

R4 berättar att de hela tiden har kurser men att de inte har någon obligatorisk kurs specifikt inom GDPR eller integritet. R4 nämner dock att om man vill lära sig mer om till exempel GDPR specifikt finns det absolut möjlighet att bli skickad på en sådan kurs, om man ber om det, men att det borde vara allmän kunskap eftersom lagen alltid är aktuell på nyheterna. Den sista respondenten, R3, svarar att de inte har några utbildningar relaterade till GDPR. R3 menar att de har en grupp som arbetar med det men det är inget som har kommunicerats ut brett på bolaget ännu. R3 erkänner även att han inte har så bra koll på GDPR som sådan.

4.3 Interna policys

Tre av fyra respondenter berättar om policys som handlar om att de ska efterfölja GDPR, eftersom det är lag. Den fjärde, R3, talar om att de fått riktlinjer angående att de ska kunna radera data ganska omgående om det skulle behövas och det har de satt upp procedurer för att göra, men inga mer övergripande policys.

O1:s moderbolag har högnivåpolicys kring personuppgiftshantering och informationssäkerhet, sedan är det upp till O1 att konkretisera och applicera det på verksamheten. R1 menar att det är svårt att skriva policys som är direkt applicerbara på projekten som levereras eftersom det är en mångfacetterad fråga. Även om de uppfyller alla GDPR:s krav när det kommer till laglig grund, biträdesavtal, dataminimering med mera, måste de se till att de håller informationen och sina utvecklingsmiljöer säkra från intrång och läckor. Därför menar R1 att personuppgiftshanteringen går hand i hand med informationssäkerheten. Förutom dessa har O1 också tydliga bestämmelser för vad man får lov och inte får lov att göra på olika nivåer, exempelvis måste R1 vara med initialt i alla projekt om de hanterar personuppgifter för att säkerställa att det görs rätt. Dessutom har O1 ett verktyg specifikt för intern regelefterlevnad av GDPR och digital integritet, där de sprider tekniska och juridiska nyheter för att hållas uppdaterade.

R2 berättar att GDPR-efterlevnad är sammanknutet med deras ISO 9000 certifiering och att det tidigare fanns motsvarande med PUL. Förutom detta berättar R2 att de har en separat kommunikationskanal för att hantera GDPR frågor eller incidenter så att det kan hanteras snabbt och effektivt.

R4 berättar att de har väldigt starka policys när det kommer till "privacy" men de som presenteras är egentligen inget som handlar om digital integritet eller personuppgifter, förutom att de ska följa lagen. R4 presenterar dock väldigt starka policys när det kommer till säkerhet.

4.4 Utvärderingar av risker

På frågan om de utför riskutvärderingar på sina system berättar tre av respondenterna att de arbetar med det, fast inte på ett strukturerat sätt. R1 berättar att han i början av ett projekt är med och diskuterar datan som ska behandlas i systemet för att se till så att det går rätt till. Men påpekar även att om de ska arbeta med känsliga data, är det inte deras ansvar att hantera detta, utan det är kunden som har det yttersta ansvaret. R2 menar på att de arbetar delvis med det, men det är lite olika från projekt till projekt. Han påpekar också att det har med kunden att göra. Att *"Det är svårt att svara på, på en generell nivå. För att det är lite, dels från projekt till projekt. Men också, har vissa kunder mer risktankar jämfört med andra. [...] Svaret på frågan är egentligen, ja det gör vi, men i olika grad beroende på. Det handlar också om att det finns en minsta nivå och sedan finns det ju hur mycket pengar man kan tänka sig betala för det."* (Appendix B, #32). R2 fortsätter att han dock inte har varit med i ett projekt där de gjort någon djupare analys med syftet för att samla informationen.

R3 berättar att det är mer en ad-hoc-fråga, när man stöter data som kan uppfattas som att falla under personuppgifter, då startar någon slags diskussion. Han säger även att de möjligtvis har någon liten process för hur det ska hanteras och att det kanske borde skapas. Han påpekar dock att det borde vara på någon slags arkitektroll som behandlar detta tidigt i processen.

Tyvärr misstänker vi att R4 missuppfattade vår fråga och gav oss ett svar som inte går använda på denna punkten.

4.5 Datasäkerhet och dåliga designer

Alla respondenter jobbar på ett eller annat sätt med datasäkerhet och att säkerställa en lämplig nivå av säkerhet. R1 nämner att arbetet med säkerhet inte har med personuppgifter specifikt att göra samt att det gjordes redan innan GDPR.
"Det är klart att det är dumt för individerna om vi läcker personuppgifter, men det kan vara dumt om vi läcker annan känslig information också, då menar jag affärskritiska eller känsliga uppgifter på så sätt." (Appendix A, #28).
Alla respondenter berättar även om att de använder sig av "code reviews" eller "pull-requests", alltså att en eller flera utvecklare granskar kod som andra utvecklare skriver innan den går in i produktionsmiljö. Detta beskriver alla som en metod för att höja kvaliteten på koden och täppa till misstag eller tankefel hos en utvecklare. Tre av fyra nämner kryptering som en av teknikerna de använder för att säkra information, även om R3 är självkritisk och anser att företagets krypteringsstandard är för svag.

R1 och R4 talar om säkerhetsgranskning av hela systemen, O1 har lagt upp det på så vis att de alltid rekommenderar kunderna att köpa en extern granskning för att upptäcka brister eller saker som de inte tänkt på. Organisation 4 (O4) har istället anonyma interna granskningar
"Typ om vi gör en deployment till produktion så har vi ett annat team som går till systemet, vi vet aldrig vem från O4 det är, de kanske sitter i Sverige, kanske i Indien, som folk sitter och gör olika test. Performing tests, hacking tests och så och efter en månad eller två veckor så får vi ett resultat. "(Appendix D, #72).
Även R2 och R3 talar om tester, men i deras fall är det inte en extern grupp som utför dem utan det är enhetstestning, automatiska tester och manuella tester men det är utfört inom teamet.

R4 talar överlägset mest om säkerhet, det genomsyrar hela intervjun. Eftersom de jobbar med till exempel banker så är det höga krav på säkerhet, dels i utveckling och dels i mer eller mindre alla delar av arbetet *"Allt, allt från hur jag dricker vatten när jag pratar med dig till var datorn ska ligga, vilken nivå av encrypting."* (Appendix D, #62). R4 menar att det är många som talar om säkerhet men det är inte så många som faktiskt lever upp till sin policy eller vad de säger.

4.5.1 Kostnader

Likt med riskerna framhäver respondenterna kostnader som en av de stora begränsningarna när det kommer till kvalitet och säkerhet.
"Med security måste man hela tiden utveckla vidare, och där har vi problem med kunderna, nästan alla. Nästan ingen vill satsa på security. [...] när det kommer ett kostnadsförslag så säger de "nja, kanske, vi får se"." (Appendix D, #54)

4.6 Påverkan i systemutvecklingsprocessens olika delar

Två av fyra respondenter, R1 och R4, säger att den del av systemutvecklingsprocessen som påverkats mest av kraven är framför allt i kravinsamling och kravanalysen. Det största problemet är att får kunden att förstå vad de vill ha och hjälpa dem formulera det. R1 nämner även att "*...vi har inte så mycket mätbara förändringar, men medvetenheten har höjts. Det påverkar förhoppningsvis slutresultat, i form utav att vi bygger förhoppningsvis bättre mjukvara. Men inga konkreta saker som är lätt att peka ut.*" (Appendix A, #58).

R4 säger att utvecklarens jobb påverkas inte så mycket utan det är den som har designat lösningen som har huvudansvaret och att utvecklare inte har den rollen för att tänka på integritetsfrågor. R4 påpekar att om utvecklarna upptäcker något så får man går tillbaka till designen och ändra i den. Denna ändringen måste sedan gå tillbaka till kravställningen och ändras där. R1 menar också att så fort krav- och designdelarna är klara är de andra stegen ganska enkla.
"Ur ett tekniskt perspektiv är privacy ganska enkelt. Att radera efter en viss tid, se till att ingen hackar sig in, använd bara informationen till bara det den var avsedd för att användas till. Det svåra är att få företaget som använder applikationen att göra det korrekt. Jag skulle säga att tekniskt är det inte så fruktansvärt svårt. Olika nivåer av kryptering eller så, det blir inte jättemycket mer avancerat än så. Men kravarbetet och få kunden att förstå, det kan vara hur avancerat som helst." (Appendix A, #50)

R3 har ett annat arbetssätt då de lägger över ansvaret på kunden och att det borde redan ha blivit identifierat. Dock under intervju nämner han att *"Jag kan ju hålla med om att det tänket borde finnas hos oss för det är ju rätt många gånger som man har beställt en integration eller har sagt att vi ska göra si eller så, som kanske inte har det här tänket. Då skulle vi ju kunna vara liksom en, inte en bromskloss, men en spärr där för att säkerställa att den här typen av data kanske inte är lämplig att använda på det här sättet."* (Appendix C, #26). R3 nämner även att tänket på privacy borde börja redan i kravinsamlingen i så fall och i integrationsarbetet är det generellt inte så mycket tanke på GDPR idag och att de har idag inga krav på sig från verksamheten. Utöver det, är den enda förändringen som R3 nämner, att

de har en lösning som de har behövt bygga om och lägga till lite funktionalitet för att få GDPR-compliance.

R2 ser heller inga större förändringar i sitt arbete, mer än att det är kravställarens ansvar över vad som ska göras eller inte.

4.7 Slutanvändares rättigheter

4.7.1 Insamling av data

Respondenterna litar i stora drag på att kunderna sköter bitarna när det kommer till syften och minimering av data som samlas in och gör inga egna analyser av det.
"[...] i alla fall när jag varit med har vi inte gjort någon ytterligare analys av syftet med att samla information." (Appendix B, #34)
"Inte i nuläget, utan det är ju lite det där med separation of duties, om det ligger på oss?" (Appendix C, #28)

Dock så nämner två av fyra respondenter att om det är något uppenbart fel eller olagligt så lyfter de frågan till diskussion.
"Det är klart att om vi ser någonting som är jättemärkligt att "oj, varför använder du datan på det här sättet?". Det är klart att vi har en diskussion" (Appendix A, #22)

4.7.2 Datas livslängd

Än en gång lyfter respondenterna att det inte är deras jobb att avgöra exakt när data ska raderas, men att de bygger funktionalitet som stödjer det.
"Sen så hjälper vi aldrig kunden med exakt om man ska gallra efter ett år? eller ska du gallra efter 10 år? Det är svårt för oss att svara på för att det är kunden som kan sin verksamhet. Vi kan så klart guida, men när det kommer till finliret, så måste det vara en jurist som får göra det." (Appendix A, #42)
"Vi bygger nästan alltid tidsbaserat, tex när någon inte har varit inloggad i systemet på X antal dagar/månader/år. Eller när en viss tidsenhet sedan någon gjorde ett köp på en hemsida etc. antingen raderas eller avpersonifieras information." (Appendix A, #38)

R4 menar att sedan GDPR är kunden tvungen att lägga en "röd tid" på all data, alltså ett datum där den ska raderas. Ett exempel R4 tar upp är om man sagt upp sin tjänst hos en bank så måste all data och loggar som är kopplade till kunden försvinna efter 5 år. Ett annat exempel är om en vårdtjänst skickar nyheter om graviditet till en individ ska mailadressen raderas två veckor efter barnet fötts.

4.7.3 Funktioner för slutanvändaren

När det kom till att bygga funktioner för rätten till att bli bortglömt, portering av data eller att dra tillbaka samtycken berättade tre av fyra respondenter att det inte var funktionalitet som kunderna än så länge inte i någon större utsträckning hade krav på.
"Den typen av funktioner finns, men oftast lägger man den som manuella typ som "kontakta oss om…". Oftast är kostnaden att bygga den funktionaliteten så pass låg och det är så pass

få som är intresserade av att använda den, att de flesta kunder och det kan många gånger också vara på vår rekommendation, men att det ska vara lätt för användaren att begära det absolut. Men det kan vara svårt på baksidan, dvs att vi kan bara hantera det manuellt. Sedan ser man hur många som frågar, är det någon som frågar varje dag, då bygger vi så klart en funktion för det. Men är det en gång om året någon frågar så är det kanske bättre att ta några konsulttimmar för att rota lite i databasen. "(Appendix A, #44)

Den enda respondenten som hade ett konkret exempel av att de utvecklat en sådan funktion var R4 som berättade att de skapat ett system för att ställa frågor anonymt, där användaren i efterhand kunde fylla i sin mailadress vilket gjorde att systemet automatiskt rensade all data som var kopplad till adressen. R3 tar upp ett exempel där de varit tvungna att lägga till funktionalitet för att slå av loggning och lägga till en funktion som rensar alla loggar för att uppfylla kraven från GDPR. Men inte att en användare själv kan gå in och rensa sin data. Både R1 och R2 nämner också exempel där de behövt hjälpa till med att radera data vid speciella fall men inte som funktionalitet för slutanvändaren.

4.8 Ansvarsfördelning

Alla intervjuobjekt är medvetna om att det inte är de som, enligt GDPR, har det slutgiltiga ansvaret för hur persondata hanteras, de levererar bara systemen eller lösningarna på tekniska aspekter.
"[...] är det ganska bekvämt för oss att, ur vårt perspektiv, ur ett juridiskt perspektiv, är det väldigt sällan det faller på vårt ansvar att definiera om kunden får lov att använda persondata på det här sättet" (Appendix A, #22)
"Mycket hamnar i slutändan på kunden ändå. Vi äger inte den koden vi skriver, utan vi levererar den till kunden som kör den på sina egna serverparker eller sitt eget moln." (Appendix A, #68)
I stora drag gör de bara det som kunderna efterfrågar och det de har fått in som krav av kunderna.
"Nej, för det finns liksom inga krav egentligen från verksamheten på det, och det är lite därifrån det måste komma. Vi styrs ju liksom av pengar, så är det ju. Är det ingen som är villig att lägga pengar på det? Nej, då kan vi ju inte utföra arbetet." (Appendix C, #42)
"Klart, det är de som betalar för det, de lägger begränsningarna "(Appendix D, #46)

4.8.1 Rådgivande roll

Tre av fyra intervjuobjekt nämner dock att de tar på sig en rådgivande roll i sina projekt eftersom de ofta har en del kunskap och erfarenheter av arbete med exempelvis personuppgifter.
"Det är inte vår skyldighet att göra det, men samtidigt vill vi vara en professionell partner som hjälper våra kunder att göra rätt. Eftersom vi har relativt mycket kunskap om personuppgiftshantering är det klart att vi försöker att, i de fall vi upptäcker, hjälpa kunden att göra rätt." (Appendix A, #24)
"Det är businessen som bestämmer, vår roll är att guida och rådgiva kunden, inte att sätta deras policys." (Appendix D, #14)
"[...]om det skulle vara något som jag identifierar som lite mer i "gråzonen", som jag, personligen tycker känns lite konstigt eller tom fel, ur ett mer etiskt perspektiv, då känner jag

mig bekväm att lyfta det, i alla fall som ett problem som behöver diskuteras." (Appendix B, #38)

Den fjärde respondenten, R3, berättar istället att de utgår från att någon från kundens verksamhet har gjort utvärderingen huruvida data är okej att samla in och behandlas. Samtidigt ser R3 att de är en tanke som borde finnas mer hos dem också:
"Då skulle vi ju kunna vara liksom en, inte en bromskloss, men en spärr där för att säkerställa att den här typen av data kanske inte är lämplig att använda på det här sättet." (Appendix C, #28)

4.8.2 Egenintresse för verksamheten

Två av respondenterna berättar också att det finns ett stort egenintresse i att skapa system av hög kvalitet både när gäller säkerhet och efterlevnad av lagar. Det är bra för affärsverksamheten att dels få nöjda kunder och dels att det inte kommer ut att de levererat något dåligt.
"Vår första punkt är att vi behöver ha glada kunder men samtidigt vill vi inte vara på marknaden som någon slags dirty spelare. "(Appendix D, #16)
"Vi vill inte utveckla någonting och se på nyheterna att någon har hackat det." (Appendix D, #58)

En tydlig skillnad från R4 och resterande respondenter är att R4 berättar att deras organisation aldrig skriver kod som de sedan bara lämnar vidare. De arbetar huvudsakligen med stora kunder och arbetar alltid långsiktigt. Miljön systemen körs i är så föränderlig, R4 tar upp webbläsare som uppdateras hela tiden som exempel, därför är utvecklingen av system ett fortlöpande projekt. Eftersom deras namn står bakom det vill de inte lämna vidare utan att göra en ordentlig "knowledge transfer" till det företag som ska ta över koden.

5 Diskussion

I kapitel fem ställs vår empiri mot resultat från tidigare forskning som introducerats i litteraturgenomgången. Materialet analyseras för att identifiera likheter, skillnader och eventuella luckor mellan vår empiri och tidigare studier på området. Efter att ha analyserat vårt empiriska material kan vi konstatera att det finns både likheter och skillnader med befintlig forskning kring utvecklares syn på, och arbete med, digital integritet.

5.1 Syn på begreppet digital integritet

På ett personligt plan delar våra respondenter grundläggande värderingar med forskarna i vår litteraturstudie när det kommer till synen på digital integritet. Alla intervjuobjekt beskriver att de värnar om sin personliga integritet när man interagerar med olika system. De är exempelvis måna om att inte bli spårade på nätet, att obehöriga inte ska få tillgång till känsliga personuppgifter eller att deras data inte ska säljas eller användas i marknadsföringssyften. En tydlig likhet med slutsatserna i Hadar et al. (2018) är att det i slutändan alltid är verksamheten och pengarna som styr utvecklarnas arbete, oavsett utvecklarnas privata och personliga övertygelser om digital integritet. Över hälften av de intervjuade utvecklarna i Hadar et al. (2018) beskriver att de går emot sina egna övertygelser kring digital integritet eftersom de är tvungna att arbeta enligt interna policys som strider mot Privacy by Design (PbD). Detta reflekteras i vår empiri, där policys i strid med PbD istället motsvaras av det faktum att respondenterna inte kan utveckla system som skyddar användarens digitala integritet om inte kunden är intresserad och beredd att betala för det.
Våra respondenter har en likartad syn som Cavoukian (2011), att det är möjligt att skapa system med bibehållen funktionalitet, som samtidigt skyddar användarens digitala integritet. Två av dem beskriver dock hur de har tvingats tacka nej till att ta sig an projekt p g a krav från kunden som bryter mot interna policys och lagstadgade krav på digital integritet. Kundens önskemål och visioner med systemen var i dessa specifika fall inte förenliga med PbD vilket i dessa fall har hämmat utvecklingen av dessa system totalt. Systemen hade kanske kunnat anpassas för att utvecklas i enlighet med de sju principerna, men som Respondent 1 konstaterar: *"Vi hade kunnat röra oss i en betydligt högre hastighet om vi inte hade haft några betänkligheter kring sådana saker. Sen hade vi fått många andra problem på köpet..."* (Appendix A, #52) Positive-sum verkar med andra ord inte vara helt oproblematiskt eller självklart.

5.2 Utbildning

Den första principen som Cavoukian (2011) tar upp är att jobba proaktivt. Utbildningar kan vara en del av arbetet mot proaktivitet. För att öka förståelsen för digital integritet hos systemutvecklare och skapa en tydligare kontext kring varför det är viktigt med att tänka på digital integritet tar Gürses et al. (2011) upp utbildning som en viktig faktor. Från de svar

respondenterna har gett på frågan om utbildning kan vi dra slutsatsen att utbildning är något som merparten, tre av fyra, har satsat på. Två har gjort det obligatoriskt vilket är ännu bättre. Endast Respondent 3 (R3) erkänner att de inte har någon utbildning i integritetsarbete och att han själv inte har gått någon utbildning samt att de inte har något krav från verksamheten på det. Detta trots att Datatilsynet (2017) nämner att det är en nödvändig förutsättning för att ha förståelse för dataskydd och informationssäkerhet vid utveckling av system. Cavoukian (2011) belyser att arbetet med proaktivitet måste komma från den högsta ledningen och förmedlas ut i organisationen för att skapa en kultur som reflekterar detta. Okunskapen om säkert arbete med digital integritet genomsyras i intervjun med R3, vilken kan ha att göra med att det inte aktivt arbetas med från högsta ledningen. Ur ett integritetsperspektiv är Organisation 4 (O4) inte helt optimalt heller. Respondent 4 (R4) berättar att medarbetarna ofta själva behöver ta ansvar och be om att få gå en specifik kurs. Eftersom utbildningen inte är obligatorisk, finns det en risk att systemutvecklare inte tar ett egenansvar och hoppar över utbildningen. Vilket i sin tur kan äventyra arbetet med en säker systemutveckling, ur ett integritetsperspektiv.

5.3 Interna policys

Danezis et al. (2014) påtalar att integritetspolicys åtminstone ska vara kompatibla med de legala krav som ställs på integritet och Datatilsynet (2017) menar att det underlättar och automatiserar säkerhetsproceduren. För att uppnå detta ska alla integritetsrelaterade policys och processer dokumenteras och vara tillgängliga för alla (Cavoukian, 2011). Trots att forskare trycker på att policys är viktiga så är avspeglas detta inte i vår empiri. Tre av fyra respondenter berättar att de endast har policys utformade för att efterfölja GDPR, eftersom det är lag. Enligt Cavoukian (2011) är detta inte tillräckligt. Cavoukian (2011) anser att för att kunna arbeta proaktivt med integritet och upprätthålla höga standarder för integritet, krävs ett tydligt åtagande som ofta är högre än gällande lagar. R3 har inte ens någon policy för hur de ska hantera integritetsfrågor utan fått lite riktlinjer för några specifika saker som radering osv, men inga övergripande policys.

R3 konstaterar att det antagligen borde finnas bättre interna policys på Organisation 3 (O3) för att främja digital integritet, men även att de som konsulter skulle kunna ta en mer aktiv och rådgivande roll i frågan gentemot kund. Respondent 1 (R1) lyfter dock att det är svårt att skriva policys som är direkt applicerbara på projekten som levereras eftersom det är en mångfacetterad fråga. Även om Organisation 1 (O1) uppfyller alla krav från GDPR, måste de se till att de håller informationen och sina utvecklingsmiljöer säkra från intrång och läckor. Därför säger R1 att personuppgiftshantering är likartat informationssäkerheten.

R4 berättar att de har väldigt starka policys när det kommer till integritet. Men de som presenteras är egentligen inga som handlar om digital integritet eller personuppgifter, förutom att de ska följa lagen. R4 visar dock väldigt starka policys när det kommer till säkerhet. Detta belyser Hadar et al. (2018) som ett vanligt fenomen hos utvecklare, att blanda ihop koncepten informationssäkerhet och integritet.

5.4 Utvärdering av risker

Alla respondenter arbetar med riskutvärderingar på olika ambitionsnivåer, men ingen av dem gör det på ett strukturerat sätt. R1 har dock ett mer strukturerat sätt än de andra, då de faktiskt lagt till en extra riskutvärdering när GDPR trädde i kraft. R1 måste nämligen vara med i början av alla projekt som berör personuppgifter och som därför faller under GDPR. Detta talar för att O1, i alla fall i någon mån, arbetar på ett strukturerat sätt med utvärdering av risker när de kommer till digital integritet, men att det yttersta ansvaret fortfarande ligger hos kunden. R2 menar att arbetet med risker ligger delvis på kunden och hur mycket pengar de vill lägga på riskidentifiering, men att de har en lägsta nivå som de ej specificerar. R3 säger tvekande att de möjligtvis har någon liten process för riskutvärdering men han nämner inte vad. Vidare säger R3 att de kanske borde skapa det för framtiden. Cavoukian (2011) och Datatilsynet (2017) menar att arbetet med riskutvärderingar bör utföras systematiskt, gärna med hjälp av ramverk och standarder, dessa ska sedan dokumenteras, publiceras tillsammans med stegen som tagits för att undvika de identifierade riskerna. Något som våra respondenter inte riktigt verkar göra, utifrån vad de själva har svarat.

5.5 Datasäkerhet och dåliga designer

Datasäkerhet är enligt Cavoukian (2011) väsentligt för att bygga integritetssäkra system. Dessutom finns det lagkrav på att den personuppgiftsansvarige ska vidta lämpliga tekniska åtgärder för att säkerställa en lämplig säkerhetsnivå, vilket ställer krav på system med hög teknisk säkerhet ((EU) 2016/679, artikel 32.1). Respondenterna ligger på två olika nivåer när det kommer till vilket fokus man har på säkerhet, R1 och framförallt R4 visar på en mycket hög medvetenhet när det kommer till datasäkerhet medan R2 och R3 inte har lika stort fokus på det. Både R1 och R4 förespråkar utförlig testning när det kommer till säkerhet och gärna att man har någon utomstående som försöker exempelvis hacka systemet. När R2 och R3 talar om testning handlar det istället endast om att testa funktionalitet, inte säkerhet. Alla respondenter argumenterar dock för "code reviews" för att höja kvaliteten på det som produceras, vilket även är något alla respondenter arbetar efter. Det stämmer bra överens med Datatilsynets (2017) riktlinjer om att koden löpande ska granskas och analyseras, även om det i våra respondenters fall inte explicit handlar om granskning ur ett integritetsperspekiv. Respondenterna nämner dels att datasäkerhet inte är något nytt i och med GDPR:s inträde och sedan handlar det om vad kunderna är villiga att betala. Respondent 4 som arbetar med exempelvis banker berättar om att de har en extremt detaljerad intern policy som styr nästan allting när det kommer till säkerhet. Samtidigt hävdar han att nästan inga kunder vill satsa på säkerhet, att det inte är någon som vill betala för det.

5.6 Påverkan i systemutvecklingsprocessens olika delar

Digital integritet ska, enligt Cavoukian (2011), vara inbyggt i designen från första början för att kunna genomsyra hela systemet och bidra till största möjliga skydd för användaren. Hon skriver: *"Privacy must be embedded into every standard, protocol and process that touches our lives."* (Cavoukian, 2011, s. 1) Det är centralt att man arbetar holistiskt med digital integritet, eftersom alla delar i processen har inverkan på slutprodukten. Hela SDLC ska med andra ord präglas av en strävan efter digital integritet. I denna fråga är våra respondenter i stort sett enhälliga och står i viss kontrast till Cavoukian (2011). Respondenterna lyfter

nämligen fram kravställning och kravanalys som en särskilt viktig del av SDLC när det kommer till att säkerställa digital integritet i det färdiga systemet.

R4 menar att utvecklaren som implementerar funktioner är på för låg nivå i organisationen för att ha något större inflytande över i vilken utsträckning användarens digitala integritet värnas. Han understryker att utvecklare inte få betalt för att tänka på sådana problem utan enbart för att implementera kraven. Trots detta kan det hända att utvecklare uppmärksammar en mjukvaruarkitekt eller tech lead på integritetsbrister som de upptäcker i systemet vid implementering. Detta är dock inte riktigt samma sak som att lägga huvudansvaret för integritetsfrågor på systemutvecklaren, menar R4. I ett sådant fall måste problemet föras tillbaka till designen så att den kan ändras och sedan vidare upp till kravnivå så att kraven omarbetas därefter. R1 sammanfattar det som att: *”Ur ett tekniskt perspektiv är privacy ganska enkelt. [...] Olika nivåer av kryptering eller så, det blir inte jättemycket mer avancerat än så. Men kravarbetet och få kunden att förstå, det kan vara hur avancerat som helst.”* (Appendix X, #50). R1s sammanfattning har tydliga likheter med Hoepman (2014), som konstaterar att det finns en hel del tekniska verktyg som hjälper systemutvecklare att arbeta med digital integritet i implementeringsfasen, men att det saknas motsvarande verktyg för designen.

De andra respondenterna delar också synen på kravställning och kravinsamling som den viktigaste delen för att säkerställa digital integritet. Detta stämmer väl överens med van Rest et al. (2012), som säger att integritetskraven bör utgöra en väsentlig del av systemkraven. När krav på integritet, säkerhet och associerade risker fångas upp tidigt, under kravställningen, så är det betydligt enklare för utvecklare att möta dessa krav och säkerställa informationssäkerhet och dataskydd genom hela SDLC (Datatilsynet, 2017) Respondenternas svar har också har likheter med Hoepman (2014) och Kallionatis et al. (2018), som framhäver designfasen som den viktigaste delen av SDLC för integritetsfrågor eftersom det är här man sätter premisserna för hela systemutvecklingen.

5.7 Slutanvändares rättigheter

Cavoukian (2011) säger att användaren alltid ska vara i fokus men det är ingenting som återspeglas i intervjuerna. Respondenterna litar på att deras kunder har gjort utvärderingarna GDPR kräver angående vilken data som ska samlas in och att de är nödvändiga för de syften som ska uppfyllas ((EU) 2016/679, artikel 5.1b, c). Endast när det ser uppenbart fel eller olagligt ut reflekterar respondenterna över användarens bästa, och även i de fallen eventuellt bara den egna kundens bästa snarare än slutanvändaren. Respondenterna förutsätter att om användare eller data finns i systemen så ska de finnas där och om så inte är fallet så är det inte deras ansvar.
Både Cavoukian (2011), Gürses et al. (2011) och GDPR säger att den persondata som samlas in ska begränsas till precis det som behövs för att uppfylla ovan nämnda syften, data får inte heller lagras längre än vad som behövs ((EU) 2016/679, artikel 5.1c, e). Respondenterna framhäver än en gång att det inte är deras ansvar att rensa data, hälften av respondenterna säger dock att de nästan alltid bygger in tidsbaserad radering. När det kommer till minimering menar R2 och R4 att det alltid är en fördel att lagra så lite information som möjligt för att minska storleken på databaser och administration, men reflekterar inte över det ur ett integritetsperspektiv.
När det kommer till faktiska funktioner för slutanvändare är det är det endast en respondent som tar upp ett exempel där de implementerat en funktion för att radera all data relaterad till

en mailadress. Återkommande är att det inte är ett krav som kunderna ställer i någon större utsträckning. Enligt intervjuobjekten är den vanliga lösningen att man skapar en kommunikationskanal i systemet där användaren kan begära exempelvis radering och sedan får det lösas manuellt. Om det skulle bli en mer vanligt förekommande begäran säger respondenterna att automatisk funktionalitet antagligen skulle implementeras i fler fall. Sammanfattningsvis verkar funktionalitet för att slutanvändare ska få större makt över sin data inte prioriteras av respondenternas kunder och därav inte heller av våra respondenter.

5.8 Ansvarsfördelning

En av respondenterna, R1, understryker att IT-konsultbolag inte själva äger den kod man producerar åt en kund efter det att projektet är klart och systemet är implementerat. I samband med att systemet implementeras övergår ägandeskapet över koden och systemet i helhet till kunden som beställt det, vilket i sin tur innebär att ansvaret för att systemet efterlever de lagstadgade kraven i GDPR också övergår på kunden/beställaren. Således känner IT-konsulterna i vår studie ett mindre ansvar för, och kontroll över, i vilken utsträckning man arbetar med integritet i ett visst projekt, då det slutgiltiga ansvaret ligger på kunden som äger och använder det färdiga systemet. Konsultbolag fakturerar konsulttimmar och utför därför inte mer än vad de får betalt för, i slutändan är det kundens önskemål och krav som styr. Varken Gürses et al. (2011) teorier om dataminimering, mönsterlösningar av van Rest et al. (2012) eller Chen och Williams (2013) riktlinjer och ramverk för implementering av PbD hjälper alltså om inte kunden är intresserad av det extra arbetet eller funktionaliteten som PbD kräver och den kostnad som det innebär.

Samtidigt ser vi stora skillnader mellan svaren från de olika respondenterna. Det faktum att man inte har ett ansvar som personuppgiftsansvarig betyder inte att konsultbolagen inte kan arbeta enligt PbD. Ett sätt att ta ansvar för digital integritet utöver lagställda krav skulle, som Gürses et al. (2011) förespråkar, kunna vara att anställa dedikerade experter på juridik och systemutveckling som arbetar aktivt med frågor om digital integritet. Samtidigt poängterar R1 att de inte är någon juristbyrå. O4, exempelvis, har enligt R4 gedigna policys och riktlinjer när det kommer till frågor som rör digital integritet. R4 och bolaget i stort verkar emellertid ha en ganska snäv bild av vad digital integritet och PbD innebär, eftersom respondenten nästan uteslutande pratar om säkerhet. Här finns tydliga likheter med slutsatserna i Hadar et al. (2018), som konstaterar att majoriteten av utvecklare sätter ett likhetstecken mellan integritet och säkerhet. Denna analys återspeglas i tre av våra intervjuer, där utvecklarna liksom i Hadar et al. (2018), pratar mycket om exempelvis säkerhet, kryptering och externa hot, medan man är mindre medveten kring andra aspekter av digital integritet är sämre.

6 Slutsats

Det huvudsakliga syftet med denna studie var att undersöka hur digital integritet behandlas i systemutvecklares arbete ett år efter GDPR:s inträde. För att uppnå vårt syfte försökte vi besvara följande forskningsfråga: "*Hur behandlas digital integritet i systemutvecklarens arbete, efter GDPR?"*

Resultatet av vår studie indikerar att systemutvecklare har viss medvetenhet kring digital integritet, men i nuläget behandlas den ej med prioritet. Vårt resultat pekar också på att de har både kompetensen och tekniken för att kunna höja prioriteten till de nivåer som litteraturen förespråkar. Ett hinder i dagsläget är att kunderna har det sista ordet när det kommer till nivå av integritet, eftersom ägandet av koden och ansvaret i slutändan hamnar hos dem. Detta faktum är även är en ursäkt som används av alla våra respondenter, vilket har tydliga likheter med studien av Hadar et al. (2018) där utvecklare tenderar att lägga över ansvaret på managers. Respondenterna tar på sig en rådgivande roll men när kunden vill ha lägsta möjliga lagstadgade nivå av integritet och inte är villiga att betala för högre kvalitet så följer IT-konsulterna i vår studie den kravställning som kunden angett.

En gemensam nämnare mellan alla fyra företag i empirin är att deras arbete med digital integritet enligt dem själva inte förändrats så mycket efter GDPR. Vidare råder det konsensus bland våra respondenter att det är i kravställning och kravanalys som integritetsfrågor lyfts, och bör lyftas, vilket är i linje med litteraturen. Fokus på integritet avtar dock i senare delar av systemutvecklingsprocessen då det lätt förväxlas med datasäkerhet.

När det kommer till aspekterna av digital integritet som avser datasäkerhet ligger dock hälften av våra respondenter långt fram och praktiserar redan majoriteten av de tekniker och aktiviteter som nämns i litteraturen. Motivationen bakom detta arbete tycks dock inte vara grundad i digital integritet, utan det är ett arbete som görs oavsett om systemen behandlar persondata eller ej, vilket också gjordes redan innan GDPR.

Trots att GDPR i skäl 78 säger att system bör utformas med hänsyn till integritetsskyddsreglerna är det fortfarande inte ett absolut krav. Många av GDPR:s krav kan lösas manuellt eller på policy-nivå, vilket företag också tycks göra. Detta strider dock mot det holistiska synsättet Privacy by Design förespråkar.

Avslutningsvis ser vi indikationer på att pengar går före arbetet med den personliga integriteten. Trots att utvecklarna personligen tycker det är viktigt med digital integritet, värderas fortfarande pengarna och verksamheten högre än samhällets och individens intressen.

6.1 Vidare forskning

Denna uppsats är, såvitt vi vet, den enda uppsats som studerar hur digital integritet behandlas i systemutvecklarens arbete sedan GDPR trädde i kraft. Vi uppmuntrar därför andra akademiker och forskare att replikera denna studie, i syfte att verifiera huruvida våra resultat och slutsatser är stämmer även på ett bredare plan. Frågan om ansvarsfördelning i IT-konsulters arbete med digital integritet är också något som vi skulle vilja uppmana andra forskare att studera vidare. IT-konsulten har en intressant roll i systemutvecklingen där det är dem som sitter på expertisen om systemutveckling och dess funktionalitet medan det är beställaren av systemet som är personuppgiftsansvarig.

Appendix A

Transkribering Respondent 1 (R1), CTO på Organisation 1 (O1).
Intervjuare: Folke Lindell (FL) och Erik Olsson (EO).
Längd 40 minuter.
Antal ord: 4480

#	Person	Meningsenhet	Kod
1.	EO	Så där, då är vi igång, trevligt att vara här!	
2.	R1	Välkomna hit!	
3.	EO	Tack så mycket.	
4.	FL	Tack så mycket.	
5.	EO	Jag tänker att vi börjar lite med dig och din roll här, vad du har för titel, vad du gör på Organisation 1, hur länge du har varit här och vad du har för utbildningsbakgrund? Om du skulle vilja berätta lite om det.	
6.	R1	Jag är CTO på O1. O1 är ett framför allt ett konsultbolag med lite över 1600 anställda. Vi finns i Sverige, Finland, Danmark, Ryssland och Polen. O1's Moderbolag är noterat på Stockholmsbörsen. Här i Skåne är vi cirka 140 anställda, varav de allra flesta är konsulter. De absolut flesta är utvecklare, projektledare eller testare. Min roll här är som CTO, vilket innebär att jag har ett helhetsansvar för all form av teknisk leverans vi gör. Det innebär oftast att överse projektleveranser i olika varianter. Både när det handlar om införsäljning och planering, stötta projektet under leveransen och sen även stötta i slutleveranserna av projekten med att gå live. Mycket är att skapa lösningsförslag hos kunder. Jag är också teamchef över cirka 30–35 konsulter. Dessutom har jag huvudansvaret för GDPR i denna regionen, i den mån någon kan ha ett huvudanvar för det, det är klart att juridiskt faller det på VDn. Men det mesta är delegerat till mig idag.	
7.	EO	Vad har du för bakgrund på O1 och utbildningsmässigt?	
8.	R1	Jag har varit på O1 sedan 2017-2018. Jag jobbade på ett bolag innan som blev uppköpta av O1. Det förra bolaget hade ungefär 20-25 anställda och som fokuserade på web och .NET. Jag gjorde ungefär samma där som här med en bakgrund som .NET och webutvecklare. Jag började på det bolaget 2013 som systemutvecklare. Innan dess har jag en kandidatexamen i Informatik från Lunds Universitet.	

9.	EO	Har du varit involverad i systemutvecklingsprojekt som har behandlat personuppgifter på något sätt?	
10.	R1	Definitivt ja, både innan och efter GDPR.	
11.	EO	Vill du beskriva något sådant projekt lite mer ingående, i den mån du kan såklart	
12.	R1	Det beror på var man lägger gränsen, eftersom vi jobbar till exempel med versionshanteringssystem så innebär det alla projekt vi gör har personuppgiftshantering i sig. Om än i ett väldigt meta-format. Vem som har gjort vad i projektet och vi har ärendehanteringssystem. Så det finns hela den biten av interna IT-strukturer, meta-projektet innehåller ju väldigt mycket av personuppgifter och hanteringen av det. Men om vi ska kolla på, jag är involverad i väldigt många projekt, men i princip alla projekt har ju på ett absolut minimum någon form av användarhantering som behöver hanteras. Det är litegrann av en praxis att vi antingen har en e-postadress eller ett AD-namn på en person, på den inloggade användaren, som systemet hanterar på ett absolut minimum. Ofta har vi betydligt mycket mer information än det. Sen har jag varit involverad i flera e-handelsprojekt som av naturliga skäl har väldigt mycket kunduppgifter. Många interna verksamhetssystem som intranät osv. har också väldigt mycket personuppgifter. Om vi tar vårt interna intranät här på O1 så har vi uppgifter om alla anställda, såsom namn, adress, telefonnummer och matpreferenser, vilket (matpreferenser) vissa kan argumentera är känsliga uppgifter osv. lite beroende på hur man vrider och vänder på det. Alla projekt hanterar personuppgifter på ett eller annat sätt, men flera stycken har lite större skala också.	DI, SR
13.	FL	Använder ni någon speciell utvecklingsmetodik på O1? Alltså om ni kör Scrum eller är det olika från projekt till projekt?	
14.	R1	Det är olika från projekt till projekt. I och med att vi är ett konsultbolag jobbar vi på det sättet som kunden vill. Sen är det klart att vi har många kunder som inte föredrar något specifikt, för att de är inga mjukvarubolag och har ingen aning om hur man utvecklar mjukvara. Det är klart att vi då rekommenderar olika metodiker. Där är det också mycket kopplat till hur avtalen ser ut. Vårt önskemål är alltid att jobba agilt, antingen enligt KANBAN eller scrum. Lite grann beroende hur förutsättningarna för projektet ser ut, men det är klart att i den bästa av världar jobbar vi agilt och jobbar i sprintar och tar betalt för sprintar så att säga. Sen är det väldigt sällan att våra kunder accepterar att köpa den typen av osäkerhet.	
15.	EO	Ok, om vi går vidare lite. Prata om begreppet ”privacy” i lite bredare termer, ”privacy” eller ”digital integritet” eller vad man ska kalla det på svenska. Vad betyder det begreppet (privacy) för dig?	
16.	I1	För mig personligen så skulle jag säga att det i första hand handlar om att jag äger min egen data, jag väljer själv vad någon annan kan se och kan göra med den. Dvs att jag äger utgångspunkten att jag kan dela ut den i givna scope till någon annan för att göra vissa saker. Men att makten ligger hos mig som användare.	DI
17.	FL	Bra svar, tycker jag. Är du bekant med Privacy by design som koncept?	

18.	R1	Ja jo det är jag ju, absolut.	
19.	FL	Och jag misstänker att du är bekant med lagar som berör integritet i informationssystem.	
20.	R1	Alltså jag har ju undervisat i PUL och GDPR. Sen finns det ju många andra också, som jag kanske har mer översiktlig koll på.	U
21.	FL	Om vi kollar på systemutvecklingsprocesser, när i processen börjar man tänka kring privacy? Alltså definierar vilka uppgifter som är personuppgifter och hur de ska samlas in och lagras etc.? När brukar det kicka igång på något sätt?	
22.	R1	När vi bygger system, bygger vi alltid system åt kunder. Vi existerar väldigt sällan i ett vakuum. Det är väldigt sällan våra system tex. har data i sig som inte finns någon annanstans hos kunden. Mycket handlar om att vi bygger system som gör någonting med data hos en kund som redan hade datan. På så sätt är det ganska bekvämt för oss att, ur vårt perspektiv, ur ett juridiskt perspektiv, är det väldigt sällan det faller på vårt ansvar att definiera om kunden får lov att använda persondatan på det här sättet. Det är klart att om vi ser någonting som är jättemärkligt att ”oj, varför använder du datan på det här sättet?”. Det är klart att vi har en diskussion, men den typen av diskussion har man ju väldigt ofta direkt på ”skisstadiet” av en applikation. Om någon kommer och vill utveckla en applikation som använder personuppgifter, så diskuterar man redan från början lite grann kring varför vi behöver denna datan, man måste arbeta med dataminimisering. Det är något vi gör ganska tidigt tex. Dessutom så kommer det upp som en naturlig del i och med att så fort vi får tillgång till personuppgifter, vilket vi ofta får som en del av utvecklingsprocessen, för att köra kunna köra testdata osv. Så hamnar vi i att vi måste ha ett biträdesavtal. Jag skulle säga att det kommer väldigt väldigt tidigt i någon form av kravarbete eller kravanalys. Sen är det klart att det kan komma utökade beställningar senare kring att ”i nästa version vill vi kunna skicka nyhetsbrev osv.” då blir det lite annorlunda så klart.	SP, SR, AF
23.	FL	Jag tänkte hoppa lite i våra frågor för att angående det här med dataminimering. Händer att ni ifrågasätter era kunder tex. ”Behöver vi verkligen dessa uppgifterna?”?	
24.	R1	Det händer absolut, sen så, som sagt, det är inte vi som är personuppgiftsansvariga. Så det är inte vår skyldighet att göra det, men samtidigt vill vi vara en professionell partner som hjälper våra kunder att göra rätt. Eftersom vi har relativt mycket kunskap om personuppgiftshantering är det klart att vi försöker att, i de fall vi upptäcker, hjälpa kunden att göra rätt.	AF
25.	FL	Du säger att ni har mycket kunskap, har ni hållit i utbildningar här internt?	
26.	R1	Jag har ju utbildat, dels alla i vår region har gått i utbildningen vid uppsamlingstillfällen ungefär en gång i halvåret. Sen har jag även undervisat åt kunder, både kunder som vi har bjudit in till kontoret. Sen har vi fler kunder som har i princip köpt en ”white labelled”-utbildning. Vi har alltså gjort utbildningar i kunders namn, för dels intern på företaget och för kundens kunder. Jag har undervisat i	U

		tyska dataskyddslagstiftningen, franska och brittiska också för att man ofta måste jämföra med vad som fanns innan. Så jag har varit runt och utbildat i ganska svenska företag och en del utländska också.	
27.	EO	Och internt, har ni på O1 policys, liknande dokument eller kanske mer informella normer hur man arbetar med privacy i era projekt?	
28.	R1	Ja det har vi. Moderbolaget har ett antal högnivåpolicys kring personuppgiftshantering och informationssäkerhet. Dem är det sen upp till mig att göra mer konkreta och applicera på hur vår verksamhet ser upp på O1. Jag har tagit fram en allmän policy för O1 som inbegriper egentligen allting som har med informationssäkerhet att göra. Sen är det inte direkt applicerbart på de faktiska projekten vi levererar. Det är en väldigt mångfacetterad sak med det här med privacy och informationssäkerhet. För att vi måste se till att hålla informationen även om vi uppfyller saker som laglig grund, biträdesavtal, dataminimering osv. Så är det väldigt viktigt att skydda våra utvecklingsmiljöer från intrång och hur vi ser till att vi inte använder mjukvaror som riskerar att läcka personuppgifter. Så egentligen går personuppgiftshantering väldigt tätt ihop med informationssäkerhet. Det är klart att det är dumt för individerna om vi läcker personuppgifter, men det kan vara dumt om vi läcker annan känslig information också, då menar jag affärskritiska eller känsliga uppgifter på så sätt. Förutom policyerna då, finns det även en massa bestämmelser kring vad man får lov och inte får lov att göra och vilka beslut vilka nivåer i företaget får lov att ta. Som exempel behöver jag vara inblandad initialt skede i ett projekt, första gången det blir att vi hanterar personuppgifter åt en kund. Då behöver jag vara med och se över det initial för att säkerställa det. Det finns även viss skriven dokumentation.	IP, DS
29.	FL	Förmedlas den dokumentationen till kunderna också? Vet de om att den finns?	
30.	R1	De vet om att den finns, de flesta, men målgruppen är internt. Den är så bred att den nog inte hade varit så relevant för så många kunder. Däremot händer det ofta att vi hänvisar till den när vi berättar om hur vi arbetar med säkerhet. Tex. Att vi har vissa krav och att utvecklare har gått en utbildning.	SR, U
31.	EO	Har ni några etablerade metoder för att identifiera risker eller dåliga designer när det kommer till privacy-problematik eller är det med ad-hoc?	
32.	R1	Vi rekommenderar till exempel alltid våra kunder att köpa en extern säkerhetsgranskning av applikationen vi levererar som en del av leveransprocessen. För att både vi och kunden har ett intresse av att, även om vi så klart tycker att vi är väldigt duktiga på det, kommer det alltid finnas saker som man inte har tänkt på eller inte upptäcker. Därför rekommenderar vi att göra en extern säkerhetstest av alla applikationer. Det görs inte i alla fall, men det görs i många fall. Annars har vi våra rutiner för att upptäcka den här typen av saker är att vi arbetar med kodgranskning i projekt. Det är aldrig en utvecklare som kan göra en ändring och att den går igenom direkt. Utan den granskar alltid av en annan person. Det är absolut ingen	RI, DS

		hundraprocentig säkerhet i det, men tanken är att fånga upp, bland mycket annat, den typen av problematik.	
33.	FL	Görs det löpande medan man skriver koden?	
34.	R1	Vi jobbar mycket med dela upp projekten i småärenden. När man är färdig med ett ärende, lämnas alla commits som hör hemma i det ärendet in för kodgranskning med stöd av Git. Tanken med kodgranskning är att dels kolla på att koden är läsbar och logisk utifrån en massa parametrar. Sedan kollar kodgranskaren om koden löser problemet som ärendet hade och gör en allmän sanity check. Detta är något som höjer kvaliteten väldigt mycker ur en massa olika perspektiv.	RI, DS
35.	FL	Gör ni några specifika riskutvärderingar, hur känsliga personuppgifterna är, vilka risker det skulle vara? Om ni behandlar uppgifter olika på något vis?	
36.	R1	Ja det gör vi, men inte på ett strukturerat sätt. I och med att jag alltid är med initialt i ett projekt när vi diskuterar vilka personuppgifter systemet kommer behandla. Det är väldigt sällan vi behandlar känsliga data, så som kredituppgifter osv. Det har man alltid tredjepartslösningar för. Ibland behandlar vi sjukdomshistorik och sådana saker. Sen ska det också sägas att så fort våra konsulter arbetar med känsliga data, gör de det i kundens regi. Då är det inte vårt ansvar att hantera alla frågor kring tex. privacy, då är det som sagt kundens. Det är när vi har en helhetsleverans mot kunden som det blir aktuellt. Sedan GDPR skedde och sedan jag har varit här, har vi inte haft några högkänsliga ur privacy perspektiv. Vi har haft högkänsliga ur affärsperspektiv, men det är alltid en säkerhetsbedömning. Vilken typ av säkerhet behövs i den här applikationen och på vilka sätt kan vi skydda informationen som finns här. Och det är som allt annat, det kan man göra på massa olika sätt. Hur arbetar vi med rätt autentisering, hur arbetar vi med intrångsdetektering osv.	RI, SR, AF, DS
37.	EO	Har ni specifika metoder eller tekniker för att hantera datans livslängd? Om man till exempel rensar datan automatiskt när den inte längre har ett syfte att fylla?	
38.	R1	Ja, för interndata har vi det. Där finns policy för varje enskild typ av data och varje lagringsställe osv. finns det en policy för hur länge den ska bevaras. Intern information är väldigt relaterad till anställningskopplad information. Den är, jag kan inte i huvudet, men det är ganska lång tid innan vi gallrar den. Baserat på att vi vill kunna ge ut arbetsgivarintyg eller liknande, vill vi kunna ge den ganska lång tid efter den har slutat. Det är klart att man kan invända, men grunden för att vi gör det är en intresseavvägan. Så det kan man invända mot om man vill det. När det kommer till kundernas så är det något vi påtalar, men i grund och botten är det kundens ansvar att ta ett beslut kring hur länge. Vi bygger nästan alltid tidsbaserat, tex när någon inte har varit inloggad i systemet på X antal dagar/månader/år. Eller när en viss tidsenhet sedan någon gjorde ett köp på en hemsida etc. antingen raderas eller avpersonifieras	SR, IP, AF

		information. Det är väldigt ofta den anonymiseras på något sätt. För att behålla statistik intakt.	
39.	EO	Som konsultbolag, har ni sett någon skillnad det senaste året sedan GDPR trädde i kraft i kundernas inställning? När de kommer och vill ha ett projekt från er, att de tydligt specificerar vad de vill ha eller är det mer generellt att de vill vara GDPR-compliant, sedan är det upp till er att fixa och utvärdera vad det innebär?	
40.	R1	Det är såklart väldigt varierande, men jag skulle säga att genomsnittskunden har väldigt dålig koll på GDPR generellt sätt. Oftast har man i kravspecifikationen bara skrivit att den ska vara GDPR-compliant, men de förstår nog inte riktigt själv vad det innebär. Sen finns det å andra sidan andra kunder som är jätteduktiga på det. Men de var å andra sidan antagligen duktiga på det redan innan också. För de har interna revisionsfunktioner eller något som gör att de har interna krav på sig att uppfylla. De har antagligen varit duktiga på det hela tiden. Jag skulle säga att den absolut största merparten har bara en abstrakt idé om att ”vi ska uppfylla GDPR och det är något som någon annan får hjälpa oss med”.	DI, SP
41.	FL	Behöver ni då gå in och kolla på syfte med behandling, vilken data som ska samlas in, eller överlåter ni det till att de ska ta in jurister för att kolla det?	
42.	R1	Nja, alltså det är egentligen upp till kunden. Vi kan ju så klart guida dem med det, men vi är inte ett juristkonsultbolag. Vi är ett IT-konsultbolag, det är klart att vi har viss kompetens på det. I grund och botten när vi får den typen av krav att vara GDPR-compliant, då förklarar vi för dem att det inte är en box man kan checka i. Det är inte så att, om vi fixar ”dessa sakerna” (GDPR-compliance) så är allting frid och fröjd. ”Ni (kunden) måste fortfarande jobba med att varför finns datan här, hur länge ska den finnas?” osv. För att det inga svart och vita svar på det. Ofta blir det att kravarbetet måste bli bättre och det hjälper vi kanske kunden med. Sen så hjälper vi aldrig kunden med exakt om man ska gallra efter ett år? eller ska du gallra efter 10 år? Det är svårt för oss att svara på för att det är kunden som kan sin verksamhet. Vi kan så klart guida, men när det kommer till finliret, så måste det vara en jurist som får göra det.	SR, AF, SP
43.	FL	Det här med slutanvändarens rätt till att ta del av sin data och rätt till att ta tillbaka sitt samtycke osv. Har ni blivit påverkade och behövt bygga om moduler för sånt?	
44.	R1	Ja det har vi gjort. Sen ska det sägas att där är det lite sisådär med regelefterlevnad bland många kunder, kan jag väl tycka. Den typen av funktioner finns, men oftast lägger man den som manuella typ som ”kontakta oss om…”. Oftast är kostnaden att bygga den funktionaliteten så pass låg och det är så pass få som är intresserade av att använda den, att de flesta kunder och det kan många gånger också vara på vår rekommendation, men att det ska vara lätt för användaren att begära det absolut. Men det kan vara svårt på baksidan, dvs att vi kan bara hantera det manuellt. Sedan ser man hur många som frågar, är det någon som frågar varje dag, då bygger vi så klart en funktion för det. Men är det en gång om året någon	SR

		frågar så är det kanske bättre att ta några konsulttimmar för att rota lite i databasen. Det beror väldigt mycket på situationen så klart.	
45.	FL	Så att det är inte så att ni har utvecklat moduler som ni kan återanvända för att just uppnå	
46.	R1	Nej, och det hade vi nog aldrig kunnat göra eftersom allt vi bygger är helt special till alla kunder. Det finns liksom inga gemensamma nämnare mellan två system egentligen. Sen hade det varit svårt att skapa något återanvändbart.	
47.	FL	Hur arbetar ni internt för att hålla er uppdaterade med senaste teknologi ur ett privacy perspektiv?	
48.	R1	Vi har ett verktyg vi använder för vår interna regelefterlevnad, när det kommer till just GDPR och privacy. Där har vi ett verktyg där vi får lite rent juridiska nyheter och till viss del även tekniska nyheter. Annars det i princip som all annan teknik att man får hålla sig uppdaterad. Det är upp till varje enskild konsult som sådan. Men vi har olika typer av kunskapsspridande aktiviteter. Vi har en blogg man kan skriva artiklar på, vi har mycket lunchföreläsningar där vem som helst på företaget kan hålla en föreläsning om vad som helst. Det blir precis som all annan kunskapsspridning för en IT-konsult egentligen.	SR, IP
49.	EO	Vilken eller vilka delar av systemutvecklingsprocessen tycker du påverkas mest av krav på privacy om vi ser på ett lite bredare perspektiv?	
50.	R1	Det är ju kravinsamling eller kravdefinitionen, det är där det blir jobbigt. För att det stora problemet är att få kunden att förstå vad de vill eller ska beställa och att formulera det i krav som vi kan implementera. Ur ett tekniskt perspektiv är privacy ganska enkelt. Att radera efter en viss tid, se till att ingen hackar sig in, använd bara informationen till bara det den var avsedd för att användas till. Det svåra är att få företaget som använder applikationen att göra det korrekt. Jag skulle säga att tekniskt är det inte så fruktansvärt svårt. Olika nivåer av kryptering eller så, det blir inte jättemycket mer avancerat än så. Men kravarbetet och få kunden att förstå, det kan vara hur avancerat som helst.	SP, SR
51.	EO	Tycker du att krav på digital integritet eller privacy hämmar innovationen när det kommer till systemutveckling?	
52.	R1	Ja, ur ett absolut perspektiv är det klart att det gör det. Hade vi inte haft några som skrupler kring hur vi hade använt personuppgifter, så hade vi kommit längre. Det är bara att se på Kina. Jag menar ur ett rent tankeexperiment är det jätteintressant att tänka sig av att använda sig av Facebook för att i princip hålla koll på om man kan få ett banklån eller inte baserat på deras relationshistorik, hur mycket sprit de dricker eller vad som helst. Sen så ser jag enorma problem med det också. Det är klart att vi hade kunnat röra oss i en betydligt högre hastighet om vi inte hade haft några betänkligheter kring sådana saker. Sen hade vi fått många andra problem på köpet.	DI
53.	FL	Har ni känt att det hämmar utvecklingsprocessen på era projekt, om man är lite mer specifik.	
54.	R1	Ja, det har varit tillfällen då vi har behövt indirekt säga nej till uppdrag. Därför vi har förklarat för kunden att ”det är klart att vi kan	SP, DI

		göra det du beställer, men du behöver förstå att det här bryter mot regelverken". På så sätt, det är inte jättemånga projekt, men det är vissa projekt som blir omöjliga på grund utav det. Det är inga stora volymer.	
55.	FL	Men då känner ni ändå något ansvar att i alla fall att meddela att det här kommer inte vara lagligt att använda?	
56.	R1	Nej precis. Vi vill inte lura våra kunder. Vår framgång bygger någonstans på att våra kunder är framgångsrika. Det finns många aspekter av det, men vi har ingen nytta av att leverera någonting och tjäna pengar här och nu. För att de kunderna kunderna kommer förmodligen inte tillbaka. Det är bättre att meningsfulla relationer med sina kunder på lång sikt.	AF
57.	EO	Ser du några förändringar i ert arbete sedan GDPR eller jobbade ni på likande sätt innan med de tidigare privacy-regleringarna?	
58.	R1	Jag skulle säga att vi ur ett tekniskt perspektiv jobbar vi väldigt likt hur vi gjorde innan. Ur ett rådgivnings- eller kravarbetesperspektiv är det klart att det har förändrats, men det är för att kraven och verksamheten har förändrats och att kunden är till viss del mer medveten. När det väl kommer till att vi har ett väldefinierat krav, så skulle jag säga att det inte har påverkat oss jättemycket, för att vi hade rätt så bra koll på det innan också.	SP
59.	FO	Så era egna processer har inte förändrats jättemycket, utan lite utökade kravarbeten?	
60.	R1	Nej det har inte påverkats av GDPR alls skulle jag säga.	SP
61.	EO	Då har vi inte specifika frågor kvar. Det är mer en lite öppen diskussion. Om du har några tankar kring vad vi har diskutera idag, om det är någonting du skulle vilja ta upp.	
62.	R1	Nej inte vad jag kan komma på.	
63.	FO	Det vi är nyfikna på är hur mycket man tänker på privacy genom systemutvecklingsprocessen?	
64.	R1	Den medvetenheten är så klart större idag. Vi har ju förändrat vår process på så sätt att alla får utbildning i framförallt GDPR men även allmän säkerhet och integritetsfokus. Men vi har inte så mycket mätbara förändringar, men medvetenheten har höjts. Det påverkar förhoppningsvis slutresultat, i form utav att vi bygger förhoppningsvis bättre mjukvara. Men inga konkreta saker som är lätt att peka ut.	SP
65.	FO	Vet inte om vi har så mycket mer konkreta frågor, det märks att du har bra koll och att dina svar oftast svara på andra frågor vi tänkte ställa.	
66.	R1	Ja, men mycket av mitt jobb idag blir indirekt kopplat till GDPR eftersom det blir mycket avtalsfrågor. Det är väldigt ofta vi får avtal från kunder där det står att "O1 har ansvar för att sköta allt som har med GDPR att göra" fast lite mer juridiskt fackspråk. Det är dem gångerna det ofta blir väldigt intressant. För att det blir en lång resa för att få dem att mogna i sin kravställning och få dem att ta bort det ur kontrakten för att det kan vi inte acceptera. Istället få dit något konkret.	SP

67.	FO	När det kommer till att bygga ett system som uppfyller alla GDPR-kraven och sånt. Brukar det komma som en egen aktivitet i slutet att kollar så att ”Är vi nu GDPR-compliant?”. Alltså att man utvecklar allting sedan kollar man om man är GDPR-compliant eller har ni ett så pass gediget kravarbete/analysarbete i förväg så att när ni kommer till slutet så är det redan?	
68.	R1	Jag skulle säga att måste finnas med i kraven för att de enkla sakerna man kan härleda från lagstiftningen är att man ska kunna exportera information, man ska kunna bevisa samtycke och återkalla samtycke osv. Det finns ett par sådana saker som är enkla att bygga användarfall kring, där med hamnar det som ärende i vår utvecklingsbacklog. Sen finns de mer abstrakta sakerna som att jobba med säkerhet osv. men det är ofta något som vi ändå hade gjort i applikationen. Det är ingen som vill ha en osäker applikation. Det är dessutom någonting som är väldigt beroende hur applikationen hostas till exempel. Hur säker vi än gör en webapplikation om man använder en vanliga databas i grund och botten så kommer information inte vara krypterad i den om man inte aktivt har aktiverat den. Mycket hamnar i slutändan på kunden ändå. Vi äger inte den koden vi skriver, utan vi levererar den till kunden som kör den på sina egna serverparker eller sitt eget moln. Mycket av de abstrakta lösningarna måste lösas där.	SP, DS, SR
69.	EO	Har ni haft projekt där ni har gått in och gjort addon-lösningar på existerande system för att uppfylla GDPR-compliance?	
70.	R1	Ja det har vi gjort. Ofta handlar det om att kunna radera eller anonymisera en person ur ett system. Eftersom många system inte har haft stöd för det. Ofta kan det vara att det enda sättet att radera någon är att gå in och ändra det manuellt, men det blir inte en bra process av det. Då har vi i vissa fall byggt funktioner för det i befintliga system. Men de projekt är oftast väldigt begränsade. Det handlar oftast bara att köra ett databasscript på rätt sätt.	
71.	EO	Är det hos befintliga kunder på system som ni utvecklat eller kan det vara både och?	
72.	R1	Ofta är det system som vi har någon form av relation till. Antingen har vi byggt det från början eller underhållt det tidigare. Jag kan inte komma på att vi gjort det på ett system vi aldrig sett tidigare.	
73.	FL	Jag känner att vi är klara.	
74.	EO	Ja, jag med. Känner att vi fått väldigt bra svar, tack så jättemycket för detta.	
75.	R1	Om det inte är något problem för er så kan ni väl köra det anonymt ändå.	
76.	EO	Ja absolut kan vi det!	

Appendix B

Transkribering Respondent 2 (I2) på Organisation 2 (O2).
Intervjuare: Folke Lindell (FL) och Erik Olsson (EO).
Längd 44 minuter.
Antal ord: 3589

#	Person	Meningsenhet	Kod
1.	FL	Ja okej Vi kan ju börja med din roll och yrkestitel.	
2.	R2	Yrkestitel är Sharepoint specialist. Och som Sharepoint-specialist fyller jag rollerna, arkitekt och utvecklare. Men sen så jag har jobbat på lite diverse projekt så egentligen har inte bara varit Sharepoint, men det har alltid varit något webbaserat eller något som man kör i webbläsaren mer eller mindre.	
3.	FL	Och hur länge har du hållit på med det?	
4.	R2	Det är i sju år nu så jag har jobbat här på O2 i sju år.	
5.	FL	Och Vad hade du för utbildning innan du kom hit?	
6.	R2	Systemvetare, Systemvetenskap, Så Bachelor	
7.	FL	Och din roll i projekt är då arkitekt/utvecklare?	
8.	R2	Ja precis, ofta så har jag lite av en kombinerad roll, så att jag både så att säga designar lösningar och implementerar lösningar. Oftast är det också på samma projekt jag gör både och. Ibland, en tredjedel av fallen, så egentligen bara utvecklare. Då är det någon annan som designar lösningen.	
9.	EO	Sitter du för det mesta inhouse då eller har du mycket kundkontakt också?	
10.	R2	Det varierar, ungefär, eller egentligen är det alltid rätt så mycket kundkontakt. Vi jobbar generellt ganska tajt med kravställare och så. I och med att vi föredrar agila projekt, och då behöver man den här snabba återkopplingen. Vilket då innebär att man jobbar ganska tajt med kunden eller kravställaren, som ofta är kunden då.	
11.	EO	Har du varit involverad i systemutvecklingsprojekt som har behandlat personuppgifter på något sätt?	
12.	R2	Ja nästan i princip alla projekt gör det. I alla fall om man säger ur ett Sharepointperspektiv, det finns ju ingen Sharepointlösning utan en slutanvändare som är personer. Jag kan faktiskt inte dra till minnes	

		något direkt projekt som inte har någon sorts användarhantering, som jag varit med i då.	
13.	FL	Nej okej, Det är ju en bra förutsättning! Särskild utvecklingsmetodik, *nämner företagets egenutvecklade metodik*, kör ni det i alla projekt eller?	
14.	R2	Nja, inte nödvändigtvis alla, det beror ju lite vad kunden, ibland så säger kunden att "vi vill köra på vårt sätt" eller de föredrar en viss projektmetodik. Men egentligen så kör huvuddelen den här *O2's metodik*-approachen. Som är en agil metod, på så sätt att man kör sprintar, återkopplar efter varje sprint och kör retrospektiv och allt sånt där. Vilket egentligen då också med utvecklingsanknytning eller hur man, det är lite särskilt där egentligen. Om man tänker själva utvecklingsprocessen kontra projektmetodologin. De kan så att säga, röra på sig oberoende lite grann, men ändå mer, ur ett planeringsperspektiv är de ganska synkade. För att man vill, med liksom om man kör deployer eller något sånt, att det är i fas med hur man kör sprintar.	
15.	FL	Ja intressant, Okej, så här en lite mer fluffig fråga, Vad betyder begreppet "privacy" eller "Digital integritet" för dig?	
16.	R2	För mig så innebär det begreppet att jag har kontroll på mina data, det som är anknutet till mig som person. Alltså att Jag personligen också har kontroll över den informationen och att den hanteras på ett säkert sätt, som är skyddat från att bli tillgänglig för andra parter som inte har med den att göra i specifika tillämpningsområden. Som exempel, man har ju hört talas om sajter eller företag säljer vidare e-postadresser osv. Att det måste vara någonting jag måste vara medveten om och ha godkänt för att det ska vara okej. Det är väl min high-level bild av det begreppet.	DI
17.	EO	Är du bekant med begreppet Privacy by Design?	
18.	R2	Nja inte riktigt så *Väldigt tvekande*	
19.	FO	Det behöver man inte vara!	
20.	EO	Vi kan ju förklara.	
21.	FO	Ja det är ett äldre begrepp från typ 90 talet som ligger i grund till GDPR, men den har lite mer etiska grunder hur man ska tänka kring privacy under hela livscykeln. Att det inte bara ska vara något som kommer efter Och man lägger på funktioner. Utan man ska ha det i åtanke redan från början. Det kanske egentligen är dumt att säga sånt här för då kanske man för en av de andra frågor. Är bekant med lagar som berör integritet i informationssystem.	
22.	R2	Det Jag är bekant med är PUL och GDPR. De är de lagar och bestämmelser som jag har varit i kontakt med och behöver ha med mig mitt jobb. *Funderande, något tvekande*	
23.	FO	Har ni haft någon utbildning det?	

24.	R2	Ja som en del att vara anställd på O2Moderbolag. Så har man krav på sig att genomgå en GDPR-utbildning. En onlinekurs som self-service, man läser och tentar av själv via en webbaserad portal.	U
25.	FL	Fanns det något liknande innan GDPR, vet du det?	
26.	R2	Det fanns och egentligen finns, vi ett utför ju Jobb utifrån ISO 9000. Som är med processer och hur man styr verksamheter och organisationen och där är det ju så att säga styrt med PUL, allting ska vara i enlighet med de lagar som gäller vilket PUL är och var innan. På så vis fanns det styrning kring det, men jag vet inte om det fanns en uttrycklig kurs som gick att checka av att man hade de kunskaper som krävdes.	U
27.	EO	När du berättar att du kommit i kontakt med gdpr i kontexten av hur ni arbetar. Har du något specifikt exempel som du ska kunna beskriva där Det har påverkat ditt arbete i projekt eller utgjort utmaningar eller vad man ska säga?	
28.	R2	Ja, ett väldigt konkret exempel är hos en kund när de jobbade med att bli GDPR-compliant. Så var det de ville ha en lösning att om det blir en breach, att ha en notis som möjliggör att snabbt aktivera och skriva in vad det är för sorts breach som det handlar om och vilken information som hade kunnat läcka. Det var en lösning som var specifikt till för att kunna agera på en gdpr-incident på ett intranät som ett exempel.	DS
29.	FO	Du säger att ni har styrdokument som säger att ni ska uppfylla gdpr. Har ni några andra interna policys eller styrdokument eller informella normer hur ni ska arbeta med specifikt privacyfrågor?	
30.	R2	Vi har det, lite också sammanknutet tillsammans med ISO 9000, att om man identifierar, om jag skulle gå runt och komma på att det här göra bättre vad gäller tex. GDPR, så har vi en intern kanal för att kunna lyfta en sån Fråga. Där jag kan skicka in ett förslag om de problem som jag har identifierat, varpå det sen blir en dialog med en chef som driver frågan vidare. Så det gäller dels hur man kan förbättra det sätt vi jobbar på eller om jag identifierat en incident. Då har vi en separat kanal, för om jag ser en incident så måste det ska det eskalera ganska snabbt. Man vill ha så lite tidsrum som möjligt från det att det händer till att det att man agerar på det.	IP
31.	FL	I Utvecklingsammanhang, gör ni riskutvärdering då?	
32.	R2	Det är svårt att svara på, på en generell nivå. För att det är lite, dels från projekt till projekt. Men också, har vissa kunder mer risktankar jämfört med andra. Det beror lite på vad det handlar för kringliggande data, sedan är det skillnad på olika verksamheter, hur känsliga de är. Svaret på frågan är egentligen, ja det gör vi, men i olika grad beroende på. Det handlar också om att det finns en minsta nivå och sedan finns det ju hur mycket pengar man kan tänka sig betala för det.	RI, AF
33.	EO	Gör ni egna undersökningar för att kontrollera vad kunden har för syfte, alltså användningssyfte, med den data man samlar in i de här systemen?	

34.	R2	Man tänker sig att, det är lite såhär, rena konkreta insamlingssystem, tex Google Analytics, det är uppenbart man samlar användarinformation, vad de(användaren) gör eller vad som händer osv. Det är ett konkret fall. Sen så har vi i, nu går jag tillbaka till Sharepoint för att det är en central del i det jag jobbar med. Där så samlas, dokumentlistor, alla sorters listor, så ser man om jag går in och ändrar i ett dokument eller sånt där, så fastnar mitt namn där, så ser man att mitt namn fastnar där och sånt. Det ifrågasätter jag ju inte, för att det är bara en standardfunktion i Sharepoint, att man vill veta vem som varit inne och redigerat sist. Och varför jag då kom in på Google analytics tex, det behöver inte vara Google analytics, men något analytics. För det är, vad jag kan komma på på rak arm i alla fall, den enda andra insamlingsfunktionen som jag varit med om att lägga till i en lösning. I det fallet har jag inte riktigt ifrågasatt syftet med datat. Eftersom det är ganska klart utifrån vad man samlar in och syftet med en sån funktion. Så svaret på frågan är egentligen att nja *tvekande*, att i alla fall när jag varit med har vi inte gjort någon ytterligare analys av syftet med att samla information.	SR
35.	FL	Nä alltså vi tänker väl också som enkla saker som att du har ett formulär där du ska fylla i massa saker för någonting, om man reagerar “varför vi veta det här egentligen?”	
36.	R2	mm *instämmande*, det kan jag säga att som [egen/privat] person reflekterar jag över det. För att för mig som person så är privacy viktigt. Men jag har faktiskt inte kommit fram till, där jag har varit med och utvecklat i någonting, att det har varit något som har känts “iffy” eller underligt varför man skulle man veta så mycket detaljer när man samlar in mer “generell data” eller något som kopplat till något specifikt. Typ “varför ska man fylla i sitt bankkontonummer” eller något sånt här weird liksom. Det har jag inte varit med om.	SR, DI
37.	EO	Du sa alltså för dig som person så är privacy väldigt viktigt. Tror du att utvecklarens inställning till privacy spelar roll för slutprodukten?	
38.	R2	Det tror jag absolut. För att, i alla fall, dels min bild här där jag jobbar och hur vi brukar jobba, så ser jag framför mig att om jag skulle identifiera någonting som jag tycker känns eller uppenbarligen går emot någon lag, om man lyfter det som ett problem, så blir det absolut något som drivs vidare. Det tror jag absolut inte är något problem eller alltså man ignorerar inte det. Sedan som det du var inne på där, om det skulle vara något som jag identifierar som lite mer i “gråzonen”, som jag, personligen tycker känns lite konstigt eller tom fel, ur ett mer etiskt perspektiv, då känner jag mig bekväm att lyfta det i alla fall som ett problem som behöver diskuteras. Sedan blir det kanske lite utifrån, om det inte är solklart att det går emot någon punkt i GDPR eller vad det skulle kunna vara, då blir det kanske en dialog med kunden eller kravställaren, så får man se “behöver man verkligen den här informationen?”. För att det kommer ändå tillbaka till dem, kring det här med GDPR, för att om någon vill ha ut sin data, så måste det [den tveksamma datan] hänga med där också. Finns det ingen poäng med att samla in en viss datapunkt, så är det nästa fördelaktigt att	DI, IP, SP, AF

		inte göra det, för att det blir mindre administration. Om det var svaret på er….	
39.	EO	Ja absolut. Apropå det, du sa att du jobbar mycket med Sharepoint, intranät, vilket jag antar då innebär att man hanterar mycket personuppgifter relaterat till anställda, eller ja en del kanske. Har funktioner som vi kom in på tidigare som, rätten att bli bortglömd tex, finns det inbyggda funktioner för det i Sharepoint eller hur är det? Har ni behövt arbeta med sådana bitar?	
40.	R2	Det finns inga direkt inbyggda funktioner för det *tvekande*. Men sen så det som är bra att ha med sig om man tänker rent tekniskt, är att i alla fall i Microsoft-världen, har man Active Directory(AD). Som är användardatabasen som står för vilka användare som finns inom organisationen. Som Sharepoint i sin tur använder sig av för att veta vilka användare som kan logga in här osv. Sedan finns det här som heter "User profile", som är en del av Sharepoint för att hantera kopplingen mellan Active Directory och användarna i Sharepoint. Men egentligen för att svara på frågan så finns ingen, Microsoft har liksom inte pushat ut en funktion som heter "glöm den här användaren", utan det är en administrativ/teknisk aktivitet att göra det.	SR
41.	EO	Ni har alltså inte byggt egna funktioner för det, utan man manuellt plockar bort det från ADn?	
42.	R2	Precis, och sedan för man också då gå in och göra en rensning i Sharepoint. I o m att man syncar användare mellan sharepoint och AD't så man har en kopia av användaren i Sharepoint i userprofile-servicen. Sedan det till och med så pass illa att på alla sharepoint-siter finns det också en referens-kopia till den användare. Så man måste hantera väldigt granulärt, på många ställen. Så det finns ingen automatisk funktion "Glöm bort en specifik användare". Trots det så finns det väldigt specifika steg och väldigt utstakat vad som behövs göras. Så det finns både bra och dåligt. Det finns inte automatiskt men det finns klara steg hur man gör det.	SR
43.	EO	Så om en kund behöver hjälp med det så går ni in och hjälper till med det, vid behov?	
44.	R2	Ja precis. Vi kan göra det i alla fall.	SR
45.	FL	Hur jobbar ni med kvalitet av kod, gör ni code reviews eller liknande?	
46.	R2	Vi har ett par. Eller till att börja med så varierar det lite projekt till projekt och kund till kund. Lite kostnadsfråga och lite allt möjligt. Det vi tjänar pengar på, det är dels konsulter. Det är jag ibland, då är jag ute hos kund och jobbar i deras projekt och team. Där är det en helt annat miljö för mig...	RI
47.	FO	Då följer du deras…?	
48.	R2	Exakt då har de bestämmelser och jag har signerat att jag ska följa deras bestämmelser och processer och allt möjligt. Så där jobbar man på ett sätt. Sedan har vi färdiga paket. Så kunden betalar, sedan installerar vi hos dom och så konfigurerar vi. Så har de produkter där och kan	RI

		köra på det. Sedan tredje är när man har inhouse. Leveranser kan vara custom projekt där vi programmerar från grunden. Eller börjar programmerar väldigt mycket och levererar det som en custom-lösning. Sedan har vi då support, som kan vara att vi har "ärvt" tex väldigt custom lösning från någon annan firma som vi ärver sen och supportar på. Så det varierar väldigt mycket. För att svara på den frågan då, kan vi ta som exempel, när vi utvecklar våra produkter. Då har vi dels code reviews, dels Azure DevOps. Vi jobbar med versionshantering där med pullrequest. Så där blir reviews där man kollar tillsammans på en viss ändring eller pullrequest. Flera kan vara involverade i en ändring och se vad som hänt i källkoden och kan se förändringen. Även i Azure DevOps använder vi oss av funktionerna för automatiska byggen och releaser. Då är det dels, med automatiska byggen, att vi kör Linting och statisk analys av kod, man låter verktyg identifierar problem i källkod. Då kan man se, det kan vara så enkelt som att man glömt ett semikolon eller att om man gör på detta viset kan det uppstå en en logikbugg för att det skulle vara ett konstigt sätt att göra det på. Så det finns ett stort spann av saker man kan indentifiera. Sedan Automatiska tester, typ enhetstester. Vi har ingen policy eller internt krav på X antal procent coverage. Utan det är mer att det som går att enhetstesta på ett rimligt sätt, intersectat med det som känns bra att testa, alltså att ha automatiska tester för, så det blir en intersection där som kanske är någonstans, mja det är en bråkdel av all kod som vi har automatiska tester för. Så det är egentligen, det är de mer automatiska bitarna vi har. Sedan som gäller våra produkter har vi också, som en del av utvecklingsprocessen, är manuella tester. Där vi också använder Azure DevOps fast då testfunktionen. Där man planerar och styckar upp tester. Man kan välja att stycka upp det på olika sätt. Men vi brukar stycka upp det per komponent, där man lista upp massa testcase och multiplicerar det med vilka plattformar man vill testa det på. Så att man får jättemånga testcase, eftersom det oftast handlar om Chrome. I detta fallet är det vad Sharepoint online har stöd för, vilket då är Chrome, Edge, Firefox, Safari, Iphone och Android. Som gör att testfallen multipliceras till att bli väldigt många. Då har vi specifika resurser för manuella testningen, där testbesäljster som arbetar på att köra testfallen. Det är kod/teknisk kvalité vad gäller produktområdet om man säger så.	
49.	FO	Vi var inne lite på det här med att "glömma bort folk" och det var mer en manuell process. Är det någon av de här, typ om folk drar tillbaka samtycke etc, har ni börjat bygga något sånt för slutanvändaren funktionalitet. Eller kunna få ut all data om sig själv?	
50.	R2	Vi har, vad jag vet har vi inte fått det som ett krav där man vill ha en "knapp". Om man tänker sig att det vi jobbar med här är Intranät. Om du går in på ditt intranät, då är det bara konstigt om det finns en knapp "glöm bort mig". För det är egentligen en del av när jag säger upp mig att "Glöm inte att glömma bort mig". Men just "glöm bort mig" är inte något som är rimligt på ett intranät. Men däremot, rent	SR

		objektivt, kan det vara rimligt att ha en knapp “ge mig informationen om mig” eller “var finns jag omnämnd i detta systemet”. Men det är inget vi har fått krav på någon gång att vi ska ta fram. Det är lite samma sak där, om någon hos någon kund vill veta “jag vill veta alla ställen jag finns med på”, i alla fall i Sharepoint där vi kommer in, då kan vi manuellt gå in och kolla och scripta ut på alla ställen en person finns omnämnd och vilken kontext. Men det är ingenting jag har varit med om eller att vi fått in en beställning på.	
51.	EO	Och inga andra förändringar du har märkt sedan GDPR trädde i kraft?	
52.	R2	hmm… Inte i konkreta sysslor eller aktiviteter i projekt eller så, förutom det jag nämnde innan med GDPR-notisen. Och förutom att O2moderbolag har styrt upp det här med E-learning. Annars så har det inte blivit några konkreta aktiviteter vad jag vet.	SP, U
53.	FL	Förutom konkreta aktiviteter, känner du att det är någon del som har påverkats ändå. Tex kravställning eller så?	
54.	R2	Njae, inte så, inte påtagligt. Men det har nog med att göra med hur ser Intranätet och att användarna då hanteras mer centralt. Det är klart att det finns lösningar där jag varit med där kunden har en kundlista över deras kunder och där står en kontaktperson. Där hade man kunnat tänka sig att det hade varit relevant på så vis att det är personlig information som inte är intern person utan en annan organisation. Men jag har inte känt någon sort förändring egentligen på grund utav GDPR.	SP
55.	FL	Tror du att privacykrav etc hämmar innovationen när det kommer till systemutveckling?	
56.	R2	Nae, det tror jag absolut inte. Men visst tror säkert att vissa innovationer har större problem med det, utan tvivel. Om man tänker sig Twitter tex, om det hade varit en ny grej idag, tex att man ska starta twitter och sen har vi GDPR. Det är absolut att det hämmar mer än att jag har en innovation som inte har med personlig data och göra. Men så det är absolut en skillnad där. Men egentligen tror jag inte att det är så stort hinder att man inte kan komma över det. Det är egentligen inte så klurigt, och framförallt inte om man har det med sig från början. Har man med sig det från början så tycker jag inte det skulle vara så klurigt att ha med dem. Det boilar ju ner till en del funktioner vad gäller den personliga datan. Sen så klart med säkerhet och sånt, men det ska alltid ha varit en prio ändå. Jag tycker inte det är okej när min data breachas oavsett. Så svaret på den frågan är, ja det ställer högre krav på vissa innovationer, men inte till den grad att jag skulle tänka mig att den skulle vara hämmande.	DI
57.	FL	Är det något mer du tänkt på när det kommer till de frågorna vi frågat idag. Något du tycker vi borde frågat eller som du vill utveckla?	
58.	R2	Bara en ren reflektion, jag tycker det är ett intressant ämne, gdpr, eller snarare personlig data över lag. Privacy liksom. För det är ett viktigt ämne för mig personligen. En annan reflektion är att det är inte ett ämne som är viktigt för tillräckligt många personer. Jag	DI

		menar, jag kör ju tex NoScript i min webbläsare generellt för att jag vill kontrollera vilka javascript som körs när jag surfar. För att jag känner inte att jag kan lita på Internet. Inte för att jag inne på skumma sajter eller så. Många vanliga sajter har javascript som jag inte litar på. Jag har ingen facebook tex för att jag är nojjig för den sortens, eller Facebook är ju ärkefienden känns det som. Men som sagt, min känsla är att det inte är tillräckligt som tycker det är ett viktigt ämne. Men det är därför GDPR är jättebra för att det gäller många människor, i Europa iaf. Det är ett steg i rätt riktning, att det[GDPR] lyfter det [integritetsfrågan]. Att det blir en allmän grej att i alla fall vara medveten om. Det är min syn på det.	
59.	FO/EO	Tack, vi känner oss klara och tack för alla svar!	
60.	R2	Tack själv!	

Appendix C

Transkribering Respondent 3 (R3) på Organisation 3 (O3).
Intervjuare: Folke Lindell (FL) och Erik Olsson (EO).
Längd 29 minuter.
Antal ord: 4392

#	Person	Meningsenhet	Kod
1	EO	Då kör vi igång. Tack så mycket för att vi får komma hit och prata lite med dig, det uppskattas verkligen. Vi kan börja lite med din roll, yrkestitel, hur många år du har jobbat här och vad du har för utbildning.	
2	R3	Ja, min titel är systemintegratör. Vilket jag har jobbat med i sju år och min utbildningsbakgrund är systemvetare i grund och botten. Jag har arbetat främst med IBMs on-prem-plattform för integration som heter Integration Bus och de senaste åren har jag också fokuserat på Azure som är Microsofts cloudplattform. Rollen som integratör innebär att jag arbetar i en konsultroll, så jag är anställd hos Organisation 3 men blir uthyrd som konsult till våra kunder för att hjälpa med dem med integrationer av deras system, både on-premise och i molnet.	
3	FL	Så du är integrerar existerande system med varandra?	
4	R3	Ja. Om de köper in nya system eller om de har leverantörer eller kunder som har system och så. Alla systemkopplingar, både inanför och utan för bolaget, som kan tänkas behövas, arbetar vi med. Lite kort om det.	
5	FL	Har du varit involverad i projekt som har behandlat personuppgifter?	
6	R3	Ja, det har jag.	
7	FL	Vad blir din roll när det kommer till sådana frågor i sådana projekt?	
8	R3	Min roll är väl kanske att ha det i åtanke på något sätt. I många av våra lösningar, vi försöker egentligen undvika att spara ner data. Vi är egentligen mellanhanden mellan två system, man har ju oftast en datakälla och sen har man en mottagare av datan. Där är det kanske mer relevant att applicera GDPR-tänket för där kommer man faktiskt förmodligen ha ett state av datan, vid något tillfälle, att man sparar ner den. Det är väl ganska sällan som man i integrationslagret sparar data	SP, SR

		under en längre tid. Det skulle vara i loggningssyfte, för loggar vi t ex en payload eller en fil, ponera att det är från ett HR-system som skickar kanske lönedata eller kanske personlig info om personer, använder vi oss av ett loggningsramverk då så sparar vi ju faktiskt ner loggar. Dessa loggar kan ju innehålla själva datan också, för det är intressant för oss att titta på vilken typ av data som skickas. Där måste vi ju ha ett GDPR-tänk, kring de bitarna, som integratör. Var det svar på frågan?	
9	FL	Ja, absolut! När du säger GDPR-tänk, har du något specifikt i åtanke då?	
10	R3	Jag har inte så mycket egentligen koll på GDPR som sådant. Det som vi har fått riktlinjer på är väl egentligen att vi i princip ska kunna wipea (radera, reds anm) datan ganska så omgående om det efterfrågas. Så det har vi ju då fått sätta upp procedurer för att göra. När det gäller kryptering och så har vi en B64-kryptering på våra meddelanden, that's it och det skulle jag inte anse är en godkänd kryptering, om det skulle vara som ett krav (från GDPR, reds anm). Det är ingen information som vi har fått utan det som vi har pratat mest om är just att kunna ta bort datan om någon efterfrågar det. Det är väl det som vi tänker på när det gäller GDPR.	IP, DS
11	FL	Vi kan köra en sån här allmän fråga: Vad betyder begreppet privacy, eller digital integritet, för dig, rent allmänt?	
12	R3	När jag tänker på privacy, då tänker jag på… Det finns ju två aspekter av det, dels mitt privatliv: hur jag rör mig på nätet då eller privat, och hur jag gör det i jobbet. Privacy för mig privat är egentligen at… Egentligen skulle man ju inte på något sätt ha någon tracking på vad jag gör eller samla in data från mina sökningar, eller liknande. Det är ju inte definitionen av privacy för mig. När man tänker arbetsrelaterat, jag menar, jag kan ändå köpa det här med att man vill kunna radera sin data exempelvis om man slutar på ett jobb: att man inte ska ligga kvar i deras records på något sätt. Det är väl också en del av privacy tycker jag. Om man är anställd, ja då finns man väl med i system och är tillgänglig, de har information om dig. Men när man slutar så tycker väl jag att det borde vara en process att ta bort den anställda helt ur systemet. Det är väl just det där att inte känna att man blir trackad i vad man gör, var man rör sig, vad man söker på. Jag menar GPS locations och liknande, men då pratar vi kanske mer telefoner och sådär.	DI
13	FL	Är du bekant med lagar som berör digital integritet i informationssystem, typ GDPR?	
14	R3	Inte på djupet på något sätt. Väldigt light weight från presentationer som har körts ute hos min kund t ex, eller så, men inte djupt på det sättet.	
15	EO	Är du bekant med begreppet eller konceptet privacy by design?	

16	R3	Nej, det är inget som vi applicerar i vårt arbete.	
17	FL	Kör ni några utbildningar på O3 i privacy, GDPR eller så?	
18	R3	Nej, egentligen inte. Vi har en gruppering, vilket är typ en person skulle jag tro, som arbetar med det men det är inget som ännu har kommunicerats ut brett på bolaget på det sättet. Jag har inte upplevt att vi har några tydliga riktlinjer kring hur man ska tänka, eller såhär som jag ser, privacy by design och liknande. Det är inget som jag har tagit del av på det sättet.	U, IP
19	FL	Nej, det blir ju inte samma sak, alltså eftersom ni utvecklar ju inte själva systemen utan skyfflar data mellan dem, så blir det inte riktigt samma sak. Har ni några etablerade metoder för att identifiera risker eller dåliga designer i era lösningar? Dels när det kommer till säkerhet, det blir ju lite ihopkopplat med privacy i era fall.	
20	R3	Vi har ju generella designprinciper för, om man pratar säkerhet, vilka protokoll man ska använda för att överföra filer och liknande. Vi har ju en liten såhär kvalitetssäkring i form av att vi har en utvecklingsprocess där man som utvecklare sitter och utvecklar, gör färdigt tester och innan det här ska gå live har vi något som kallas för en pull request review, vilket innebär att all kod som har skrivits, innan det pushas upp till vårt master repo och faktiskt blir deploybar kod, så finns det en spärr där en eller två medlemmar i vårt team ska gå igenom koden för att se över de här bitarna. Då har vi ju en liten sådan här checklist för att man ska titta av, men i ärlighetens namn kan jag ju inte säga att vi har… Vi har en checkbox som säger “Is this GDPR compliant or not?”. Om det är det eller inte. Det är på den nivån liksom. Men sen om vi är kvalificerade att avgöra? Oftast ställer man ju en fråga till projektet som man sitter i kanske, man förväntar ju sig någonstans att kanske inte en projektledare, men en business analyst borde ha den här informationen: om det här är GDPR eller inte.	DS, RI
21	FL	Händer det någonsin att man får det negativa på den checkboxen, att man blir stoppad där?	
22	R3	Nej, för jag menar även om det är GDPR eller inte så får vi ju göra en liten assessment där på: “Okej, det här är GDPR-data som skyfflas, finns det någonting i integrationslagret, i överföringen av data, som skulle äventyra de här GDPR-riktlinjerna på något sätt? Är det någonting som vi bryter emot? Utan att vara hundra procent insatt så har jag svårt att tro att det skulle vara det egentligen. Så att det finns en liten tillstymmelse av process för det, men det är inte något vidare… Om jag gör en pull request på en kollega så har jag nog svårt att bedömma huruvida vi skulle ta åtgärder på hans kod för att comply med GDPR. Förutom om det är så att vi skulle spara ner det någonstans, då kan man ju lägga en notis om att huruvida vi har script för att kunna wipea de här grejerna. Det är på den nivån.	RI

23	FL	Det finns en del såhär i GDPR, att man bara ska använda data för det syfte den är insamlad för. Är det någonting ni, jag tänker om man skyfflar det till ett annat system så finns det ju en möjlighet att då helt plötsligt ska du använda datan till något annat.	
24	R3	Så kan det absolut ju vara.	SR
25	FL	Är det någonting ni har tänkt på? Eller det är upp till kunden?	
26	R3	Det är väl ingenting som vi tänker på så, utan ofta så sitter det någon från verksamheten som har gjort den här bedömningen att den här datan ska in i den här systemet och den ska användas på det här sätter. Så jag tror att redan i det steget så borde det vara identifierat, om det går emot GDPR. Så inte en typisk fråga som vi brukar ställa.	AF, SP
27	EO	Och ni gör inga egna undersökningar för att kontrollera vad kunden har för syfte med datan?	
28	R3	Inte i nuläget, utan det är ju lite det där med separation of duties, om det ligger på oss? Jag kan ju hålla med om att det tänket borde finnas hos oss för det är ju rätt många gånger som man har beställt en integration eller har sagt att vi ska göra si eller så, som kanske inte har det här tänket. Då skulle vi ju kunna vara liksom en, inte en bromskloss, men en spärr där för att säkerställa att den här typen av data kanske inte är lämplig att använda på det här sättet.	AF, SP, RI
29	FL	Någon slags rådgivande roll?	
30	R3	Ja, men då är vi nog uppe på någon slags arkitektroll, en renodlad arkitektroll, där man sitter och tittar på datakontrakt och datamodeller. Jag har ju en del av det i mitt jobb också. Som integratör arbetar man ju både tekniskt med implementation, men med erfarenhet så blir det ju mer och mer av en arkitektroll också men jag tror inte att en renodlad integrationsarkitekt fattar den här typen av beslut, men borde helt klart ha med sig det här tänket in när man sitter i diskussionerna med verksamheten.	RI
31	FL	Jag tänkte på det här med att du sade att ni oftast inte lagrar data i era lösningar. Händer det att ni behöver bygga ihop så att om datan försvinner ur ett system så försvinner den ur det andra? Jag tänker om vi tar exemplet med en asntälld som slutar, så finns ju hans data säkert i tio olika system. Har ni behövt hantera det, att om de wipeas från det ena så ska de wipeas från de andra?	
32	R3	Precis, det hanteras ju oftast från ett AD (Active Directory, reds anm) då. Man har ju ett centralt AD som delar ut accesser till de olika systemen, och då är det där det ska stängas ner. Jag har inte sett på några kunder jag har suttit hos att vi har byggt integrationer för att göra de här grejerna. Vi har i och för sig en integration där det handlar om att flytta användare mellan AD-grupper. Till exempel har man en AD-grupp för employees, en för leavers och en för graveyard. För	SR

		leavers då kanske de ligger kvar i ett år, potentiellt skulle man kunna bli återanställd och då plockar man bara upp den här anställde från leavers. När de går i graveyard så är de borttagna totalt. Där har vi lite integrationer som stöttar just den processen.	
33	FL	Det vi egentligen skriver om är ju själva systemutvecklingen från start to finish av system, och du kommer ju in egentligen efter att systemen finns på plats och du integrerar i dem. Men jag vet inte, vad har ni för olika steg i era intergrationsprocesser, typ hur ni arbetar i projekt?	
34	R3	Typiskt sett så inleds ju projekt med att man har känt ett behov av en integration mellan en eller flera system. Sen börjar man ju då med en kravinsamling, massa möten där man sitter och försöker hitta kraven. Där kan jag ju se att där borde det ju finnas mer GDPR-tänk än vad det finns idag. Ofta är det inte en topic för de här diskussionerna, när man tänker på integrationsbitarna. Efter det så handlar det om att ta fram en design och sen implementerar man ju, och det är en utvecklingsprocess där. Bygger man det i molnet så kanske man skriver lite functions i Java eller .NET, eller vad det skulle kunna vara och pratar vi on-prem med integration bussen så handlar det ju om att sätta upp flöden, och bygga flöden där.	SP
35	EO	Så det är ju ändå väldigt likt, det blir ju ändå en livscykel, en SDLC	
36	R3	Ja, precis. Så är det ju, helt klart. Men jag kan väl generellt säga att när det gäller intergrationsarbetet så är det nog rätt så lite GDPR-tänk idag.	SP
37	EO	Var skulle du säga att behovet är störst för ett sådant privacy-tänk i den processen liksom?	
38	R3	Ja, det är ju redan under kravinsamlingen, det är där det ska identifieras. Man kanske har vissa delar av integrationen som är känsliga. Jag menar ibland så är det ju så att vi använder oss av kanske en lookup-tabell i en databas där vi potentiellt skulle kunna ha… Vi skulle ju kanske aldrig spara ner persondata på det sättet liksom, men vi skulle kunna… Jag har gjort lite integrationer mellan ADt och HR-systemet, och där sparar vi ju ner cost center t ex och sen korrelerar vi det med inkommande, alltså, employees som kommer. Sen om det är GDPR-klassad data eller inte… För det är ju liksom ett internt cost center för bolaget.	SP
39	FL	Det skulle väl vara användaruppgifter och så.	
40	R3	Ja, och det är sällan vi sparar ner det, förutom att vi alltid gör det i vår loggning, där har vi det ju faktiskt sparat. Då har vi det ju liggande så vi har ju roterande loggar på tre månader, så tre månader bakåt kommer man kunna hitta data och då ligger den ju då B64-kodad, vilket inte då är en godkänd krypteringsmetod. Eller, det är det ju men…	DS

41	FL	Är det något som du försöker förändra?	
42	R3	Nej, för det finns liksom inga krav egentligen från verksamheten på det, och det är lite därifrån det måste komma. Vi styrs ju liksom av pengar, så är det ju. Är det ingen som är villig att lägga pengar på det? Nej, då kan vi ju inte utföra arbetet.	SP, AF
43	FL	Nej, och ni har inga kunder som specifikt frågar efter typ GDPR-tänk eller privacy eller säkerhet?	
44	R3	Inte så… Många av dem driver ju det här internt och sen om man tänker på O3 som bolag så är vi ju inte specialister på GDPR på det sättet, så vi tas ju inte in för att arbeta med GDPR på det viset.	
45	EO	Nej, ni är ju ingen juristbyrå liksom.	
46	R3	Nej, precis. Men däremot så finns det ju… Alla bolag arbetar nog med det här mer eller mindre numera men jag tror det viktiga är att det måste finnas tydliga riktlinjer, t ex i en utvecklingsprocess. Dels att GDPR ska vara med som en punkt och vad, vad klassas som GDPR? Vad ska man kika efter i utvecklingsprocessen?	SP
47	FL	Och det är inget som ni har i dagsläget?	
48	R3	Eh, jag har sett väldigt lite av det hos mina kunder, så är det.	SP
49	EO	Ser du någon konkret förändring i ditt eller O3s arbete under det senaste året, sedan GDPR trädde i kraft?	
50	R3	Ja, alltså… Det blir ju väldigt specifikt från kund till kund, tror jag. Ofta så anpassar man sig ju lite till… Jag menar vi har ju många kunder som arbetar på olika sätt. Vissa driver kanske GDPR väldigt hårt och är väldigt nitiska med det. Andra är kanske… De har gjort the bare minimum som krävs för att få compliance med de här riktlinjerna. Jag tror inte att vi har överlag ändrat arbetssätt på någon större del, det tror jag inte.	SP
51	FL	Om man har en sådan kund som är väldigt nitisk med det? Hur kan det påverka er?	
52	R3	Det kan ju påverka designen av lösningar, det kan det ju helt klart göra om man har riktlinjer för det. Det skulle ju potentiellt påverka hur man loggar, om vi kommer tillbaka till det igen, nu går det som ett jävla mantra här men det är ju det vi kan relatera till, egentligen. Jag menar, de kanske vill ha extremt bra processer för att specifikt ta en användare och bara liksom ta bort direkt och då får man ju utveckla funktionalitet för det. Det kanske t o m är så att man måste ha funktionalitet för att kunna stänga av loggning, man vill inte logga några datum ö h t och att det kommer som en riktlinje så liksom. Så där hade man ju kanske behövt göra lite förändringar, både i hur man utvecklar det och hur man tänker kring det här med loggning och monitoring.	SP

53	FL	Är det här några grejer som har hänt eller är det bara potentiellt?	
54	R3	Eh, alltså det har ju… Där jag sitter nu så har vi ju fått tänka på det här för där har vi ju en (...) lösning som vi har sedan innan som har behövt byggas om lite för att byggas om lite för att complya med GDPR. Vi har lagt till lite funktionalitet för att stänga av och slå på loggning för specifika integrationer. När det gäller att ta bort data så kan vi i princip bara gå in och trycka på en knapp så tas det bort för då en månad.	SP, SR
55	FL	Tar bort all data liksom?	
56	R3	Ja, så det är ju…	
57	FL	Men ni kan inte cleara det för en användare liksom?	
58	R3	Nej, det har vi inte processer för.	SR
59	EO	I det här senaste projektet, det var på kundens begäran som ni implementerade den här funktionaliteten?	
60	R3	Japp.	
61	FL	All right. Känner du på något vis att alla de här nya kraven på integritet, alltså och informations… Typ att du ska kunna ta bort användare och så. Känner du att det hämmar utvecklingen på något vis?	
62	R3	Nej, det tycker jag inte. Det handlar egentligen bara om att… Alltså jag menar det är väl rätt så… Jag ser det ju mer som en möjlighet att bygga en schysst lösning liksom. Du får ju en bra flexibilitet i din lösning om det är så att du kan t ex stänga av och slå på loggning. Jag menar utöver det här med GDPR-tänket så har man kanske ett gäng integrationer där det inte finns någon mening med att logga, det ligger bara och tar upp plats de här loggfilerna. Då kanske man väljer att bara logga om ett fel kastas t ex. Vi behöver inte veta varje gång det har gått bra utan vi behöver bara veta om något har gått fel här. Så jag ser det snarare som en möjlighet att kunna bygga bättre lösningar på det sättet.	DI
63	EO	Ja, speciellt om man har det privacytänket i sitt privata, eller sitt vardagsliv, så är det ju klart att det överförs på arbetslivet också	
64	R3	Ja, så är det ju	
65	EO	Så länge det inte… Sen finns det ju organisationer där organisationen aktivt har policys som motarbetar ett sådant tänk och då är det ju klart att det kan bli en clash med den enskilde anställde. Men som du säger, det håller vi ju med om också såklart, att tanken med lagen är ju att det ska vara en win-win liksom, eller i ert fall en win-win-win, alltså både för er, för kunden och för slutanvändaren. Om det görs på rätt sätt liksom	

66	R3	Ja, precis. Jag menar jag tycker inte det är fel att ha schyssta processer för just det här med privacybitarna. Det är väl bara något som man som anställd hade uppskattat, om bolaget man arbetade för hade det på plats. Sen förstår jag att det är nog väldigt bökigt för bolag som inte har de här processerna på plats, det tror jag. Framförallt om man tänker folk som arbetar med AD och det här med access management, där tror jag man har fått rodda om rätt så mycket på många bolag och göra om sina processer där för hur man hanterar anställda. Det är nog de som har drabbats hårdast om man säger så.	DI, SR, SP, IP
67	FL	Vi har inte så många fler direkta frågor. Har du tänkt något kring privacy själv som vi har missat, just när det gäller utveckling av lösningar och sådär?	
68	R3	Nej, alltså det är ju… För mig är det ju det här att jag inte vill känna att jag är loggad någonstans och det tror jag väl ändå att gemene man kan vara rätt så överens om att det är ju… Sen så ofta är det ju inga problem om någon skulle ligga kvar i ett system, det händer ju oftast ingenting med den här informationen eller påverkar det på något sätt liksom. Men det är ändå lite en sanitetsgrej liksom, att vi har kvar ett gäng på tio pers som har jobbat här i fem år, vad gör de kvar i vårt system? Varför ligger de här? Det är ju lite av en sådan sanity check på något sätt också.	DI
69	EO	Men om vi tänker mer externt med kunders kunder snarare än deras anställda, alltså typ CRM-system tänker jag att du kanske också har arbetat en del med?	
70	R3	Ja det har vi också gjort integrationer mot.	
71	EO	För där har ju alltså slutanvändarens eller slutkundens data har ju i större utsträckning blivit en råvara eller en resurs för vissa bolag. Är det någonting du har stött på? Alltså att man vill använda kundernas data som en resurs för att tjäna pengar eller så?	
72	R3	Jag kan tänka mig att man gör det. Kanske utan att vara helt öppen med det liksom. CRM-system är ju till för att bara samla in så mycket data de bara kan från kunden för att använda det i olika syften ju, försäljning eller produktion t ex. Ja menar du kan ju ha säljstatistik på att den här kunden har köpt… Om vi tar Nike som ett exempel; vi har en kund där som köper 50 skor om året. Det är klart att om man ser det liksom consecutively under tre år så är det ju klart att man börjar bygga prognoser på de här siffrorna t ex. Utifrån det så kan man skicka ner det till sin… Om man har en produktionslinje som säger att "ja vi har minst 50 skor här…" Nu är det ju ett lite förenklat exempel här, men "vi har minst 50 skor som vi ser här per år. Köp in grejer för det här nu och liksom förberedd för det." Det är ju samma typ av data som man skickar in men det är ändå två olika syften liksom. Det ena är att lägga en prognos på försäljning och det andra är att planera sin manufacturing. Sen vet jag inte om det liksom är en violation mot GDPR?	SR

73	EO	Nej, det är väl snarare om man säljer vidare den datan till tredje part, det kan ju vara ett exempel.	
74	R3	Ja, ja, okej du tänker så. Och det finns det väl många som gör, helt klart. Framförallt, det gäller ju allting egentligen, alltså ut på nätet. Jag menar du har ju sådana här som samlar in data, sökningar och liknande och säljer vidare till third party. Jag vet inte, hur ställer det sig i relation till GDPR? Så länge de informerar om det så är det okej?	
75	FL	Lite så, eller så länge ingen motsätter sig så är det ganska lugnt. Nu är ju inte vi jurister.	
76	R3	Nej, nej. Jag tänker om det är en stor punkt liksom?	
77	EO	Ja, det står ju i lagen att data bara ska användas för att fylla ett grundläggande syfte liksom. Fast sen kan du använda det för andra syften också så länge ditt intresse väger över individens intresse, vilket är otroligt luddigt.	
78	R3	Så det finns lite loopholes?	
79	EO	Ja, lite så. Och det är väl därför man ser alla de här enorma bannersen på hemsidor som tar upp halva datorskärmen.	
80	R3	"Såhär gör vi med din data, accepterar du eller inte?" Nej, men det är ingenting jag har sett ute hos kunder, inte på det sättet. Jag tror att de flesta, åtminstone större bolagen, har ju nog relativt bra koll på det här. Sen om de är liksom uppe i nirvana när det gäller GDPR, 110% compliant, nja, men de flesta har nog en baseline ändå, ett minimum på vad som krävs. Sen så, någonting som man har efterfrågat är ju kanske lite tydligare riktlinjer. Även om det inte går att applicera så bra på integrationsarbete.	
81	FL	Menar du internt eller ute i projekten från kund?	
82	R3	Eh, internt hade man i alla fall velat ha informationen, men även ute hos kunderna. För det kan ju skilja sig från kund till kund vilken typ av riktlinjer de har. Några kanske tar lite lättare på det medan andra kunder är mer nitiska och det skiljer sig väldigt mycket, hur bra de är på att kommunicera det här. Men sen är det ju som vi… Jag tror inte det är jättemycket påverkan på integrationsarbetet, med GDPR, utan det är nog i de fallen man sparar undan datan. För vi hanterar ju inte datan om man tänker på det här med att man skulle hantera datan för olika syften. Vårt syfte är att flytta data från punkt A till punkt B, sen om vi blir delaktiga som någon slags enabler då om det kommer in från källsystemet till mottagandesystemet och de använder datan på ett felaktigt sätt. Skulle det ha förhindrats i integrationslagret? Ja, kanske.	SR, IP
83	FL	Alltså, ett av problemen vi har sett från våra intervjuer är att det är ju inte ert ansvar (konsultbolagens, reds anm).	

84	R3	Nej, och det är ju lite såhär separation of duty. Det måste vara någon som egentligen kanske har det här ansvaret, för GDPR-bitarna specifikt, för att se till att säkerställa så att det sköts på ett korrekt sätt.	AF
85	FL	För alltså, om ni skulle ifrågasätta de här grejerna… Det enda ni kan göra är att rädda kunden, för ni själva behöver ju inte räddas, för ni är ju rätt safe i det.	
86	R3	Nej, precis. Och där tror jag att det finns nog en lång resa för många bolag att just hitta eller att sätta det ansvaret på en person, och det tror jag inte finns på så många bolag idag. Någon som har uteslutande ansvar… Att ner på projektnivå kunna säga att "nej, nej, nej, så här får ni inte göra, det är inte i enlighet med GDPR". Det har jag inte sett mycket av hos kunderna så där finns nog en del kvar.	AF, SP

Appendix D

Transkribering Respondent 4 (R4) på Organisation 4 (O4)
Intervjuare: Folke Lindell (FL) och Erik Olsson (EO).
Längd 49 minuter.
Antal ord: 6012
‘Vårdtjänsten’ är kund till O4 och stor svensk aktör inom hälso- och sjukvårdsbranschen
‘Banken’ är en kund till O4 och stor internationell aktör inom banksektorn

#	Person	Meningsenhet	Kod
1	EO	Sådär då är vi igång	
2	R4	Ja det är lugnt. Jag jobbar som solution architect jag är lite combo, ibland utvecklar jag också. Jag har börjat med utvecklingsbakgrund. Jag är solution architect med du kan höra mycket, det finns massa olika architect men det är endast solution architect som är hands on code. De andra, enterprise architect, delivery architect och så sitter högst. Solution architect det är hands on code, de enda som pratar direkt med utvecklarna. Jag har varit solution architect med Vårdtjänsten och från början av året flyttade jag till Banken. Vi var inte ansvariga för läckan, jag vet inte om ni har läst det?	
3	FL & EO	Jo	
4	R4	Ja, det är inte vår del, det är bara webben som är vår del. För att jag fick mycket samtal och så av gamla kollegor som undrade hur det gick så men jag kunde inte svara. Det var inte O4s ansvar, det var en helt annan firma. Ja GDPR det beror på, den är stor GDPR, det är inte någonting nytt, den fanns men det var ett extra tryck från EU för att firmor skulle börja tänka på sån privacy issues. För att på den gamla tiden, speciellt de telefonsäljarna och så, sålde hela tiden deras kunddatabas. Du har ett kontrakt för 2-3 år även om det slutat de vet vad du tycker om och sånt, så den databasen har de hela tiden sålt vidare. Privacy är inte bara för en person, även firman kan ha privacy, kanske man har ett B2B kontrakt med en firma, men efter man har bytat vill du inte att de behåller din information. Man vet inte, de kan sälja den eller någonting och det är därför det blir extra tryck på det.	DI

5	FL	Redan spännande! Okej, vi kan börja med hur många år du har jobbat med systemutveckling och vad du har för utbildningsbakgrund?	
6	R4	Ja, jag har två masters från Malmö Högskola, en Software Engineering och den andra är Computer Science, 2010 och 2011.	
7	FL	Har du jobbat här på O4 sedan dess?	
8	R4	Ja, jag började som helt grön.	
9	FL	I de systemutvecklingsprojekten du är involverad i, brukar det vara personuppgifter inblandat?	
10	R4	Ja absolut, när du börjar utveckla finns det inga personuppgifter men sen när systemet är igång det är då det hela tiden finns. Det beror på när du är systemutvecklare. Vi säger att du ska utveckla ett system som tar kunder, du utvecklar ett fakturaprogram. När du är en stor firma har du en process. Du har en development miljö, en testmiljö, en UAT miljö och du har produktionsmiljö. Development miljön är den som utvecklarna jobbar på, testmiljön är när utvecklarna har utvecklat och det går vidare till test och sen UAT är där kunderna kundtestar. Det finns privacy när du inte kan flytta kundinformation även om det inte fanns GDPR. Kunden har rättigheten att det bara är den firman som håller deras information, om det finns en underkonsultfirma, typ att O4ini utvecklar till ett annat konsultföretag till exempel. Så det är ett annat företag som kommer behandla kundinformationen. Hela tiden när vi flyttar databasen måste vi tänka på att hasha eller ta bort viktig information, eller byta ut namn och personnummer. När man börjar utveckla kommer man inte tänka på om det finns kundinformation eller inte, men sen när man flyttar databasen om det blir error i produktionen och du vill se hur det ser ut i din miljö. Det är när man flyttar databasen man inte kan ta ner databasen “as it is” när du blandar kunder. Detta var innan GDPR, efter GDPR har det börjat bli lite annorlunda. När du utvecklar måste man tänka från första punkten hur man hanterar kundinformation, absolut. Men utvecklare behöver inte tänka så mycket, det måste hela tiden vara en teamleader eller någon som designat. Utvecklare kan ge input men det är hela tiden den som har designat systemet som har huvudansvaret för hur user information kommer att sparas och tas bort.	RI, SP, SR
11	FL	Så det är alltså den rollen du har som arkitekt?	
12	R4	Ja. Jag vet inte hur mycket frågor ni har men vi hade ett ärende med en bank. GDPR reglerna säger att banken kan hålla kundinformation max fem år efter att kunden har slutat. Om du slutat från Nordea kan Nordea hålla din information i fem år. Men, interna policys på banken säger att de måste hålla kundinformationen i sju år på grund av redovisning för skatteverket. Det blir regler ovanpå regler, vem är starkare? GDPR regler är nyare men det är deras legacy regler. Om du går hela vägen till court, det de säger är att systemet måste hantera	SR, IP

		sånt men du behöver inte hantera. Det är typ som att du har en pistol hemma, men du får inte använda den. När du utvecklar måste du tänka på hur du kommer hantera right to be forgotten, men banken har rätten att neka och säga "nej vi kommer inte ta bort din information, vi måste hålla den i sju år" på grund av att de har legacy policys som säger det och de är starkare än vad GDPR säger. Men det är inte hela tiden, de måste redovisa varför, här har de en stark punkt på grund av skatteverket.	
13	EO	Och då lyssnar ni på kundens krav?	
14	R4	Ja det är businessen som bestämmer, vår roll är att guida och rådgiva kunden, inte att sätta deras policys. Jag måste förstå deras policys men jag är inte advokat eller legal, jag bara följer reglerna som jag läser men jag vet inte hur man kan gå runt reglerna. Om kunden säger att jag vill ta bort min information har man 72 timmar om man är ett vanligt företag. En bank har en månad på sig att ta bort den. Jag ger den informationen till kunden men deras business kommer med ett svar till mig "nej, vi förstår det men du behöver inte tänka på det pga den punkten". Min roll är att rådgiva men jag kan inte bestämma över dem, de betalar, vi följer vad de säger. Men vi har rätt att anmäla dem om de inte följer reglerna. Om de hela tiden säger att de inte kommer att följa den punkt slut. En vanlig utvecklare kan anmäla, du kan anmäla banken, det är friheten i Sverige. Man kan lägga frågan till mig varför, så kan jag fråga kunden, men utvecklarna kan inte fråga kunden direkt.	AF
15	EO	Är det lagen som säger att ni ska anmäla eller är det O4s policy som säger det?	
16	R4	Det är blandat, det är O4s policy på grund av att vi följer vad lagen säger. Men absolut, vår första punkt är att vi behöver ha glada kunder men samtidigt vill vi inte vara på marknaden som någon slags dirty spelare. Vi följer hela tiden, vi har training, background check, allting, alla som jobbar för bank jobbar så. Bankinformation det är private sector I public sector, Vårdtjänsten, om vi hade en som ringde och sade "Jag var gravid förra året men fortfarande får jag gravidnyheter, hur har ni min mailadress? Varför har inte systemet tagit bort den?". Vi har 72 timmar. Om det inte går inom 72 timmar kan kunden bli anmäld till Datainspektionen och få böter.	IP, AF, U
17	FL	Har ni interna utbildningar på O4 för att lära sig om GDPR eller andra lagar?	
18	R4	Vi har inga i Malmö, men vi har hela tiden kurser. Om någon utvecklare kommer till en chef och säger att de vill lära sig mer om GDPR absolut, då säger vi att de kan hitta något eller att vi hittar något så skickar vi dem på kurs. Men den lagen kommer alltid på nyheterna så man kan läsa där. Vi har "itslearning" på O4 som är typ som ett universitet så det finns hela tiden sånt. Men vi har inga kurser där folk kommer och berättar, kanske i framtiden, jag vet inte.	U

19	FL	Ni agerar rådgivande för kunden i personuppgiftsfrågor, har ni interna policys för hur ni ska rådgiva?	
20	R4	När man rådgiver måste man komma med ett förslag, när jag säger att "du får inte spara kundinformation i fem år" måste jag komma med ett förslag hur vi ska hantera det. Inte bara ett förslag utan även varför det är bättre för kunden, det finns böter, vi kan inte bara säga att "lagen säger så". Hela tiden måste vi komma med ett förslag. I slutändan ger vi all information till dem och de får välja om de vill göra ändringar eller inte. Om man har en liten kund är GDPR enkelt att hantera men om man har en stor kund är det inte alls enkelt eftersom det systemet inte bara är ett system utan massor av system som pratar med varandra och det är ett stort arbete.	AF, SP
21	FL	Har ni etablerade metoder för hur man identifierar dåliga designer eller risker när det kommer till just privacy frågor?	
22	R4	Privacy frågor, det har vi, hela tiden har vi en person som är specialist på att hacka information, typ hacker. När vi går till produktion eller innan det, sitter de med oss och vi säger "okej, hacka detta systemet". Då visar vi vad som är starka punkter och så, om vi har gjort en transaktion mellan två system - "här kunde jag hacka" - "varför kunde du det?" - "det är inte https eller certifikationer eller krypterat så bra" Så det finns hela tiden testare, de ena är hackers som vill krascha eller hacka systemet och logga in. En annan privacypolicy är lösenord, vi är mot att någon skriver in egna lösenord, det är viktigt. På grund av att det spelar ingen roll hur starkt du har gjort ett system, det räcker med en person som inte följer de reglerna så är man genom väggen och inne. O4 provar bäst hela tiden det finns policys och hela tiden varje vecka kommer det någon mandatory kurs och efter det skriver man exam. Men man vet inte, du kanske svarar på ett sätt men på riktigt gör du inte så. Typ om du har en dator och du går och tar en kaffe, även om det är låst dörr får du inte göra det utan att låsa datorn och hårddisken ska bli krypterad.	RI, IP, DS
23	FL	Så ni har väldigt starka security-policys?	
24	R4	Ja, vi har även två stegs authentication när man loggar in i VPN:en, vi har en dosa, som när man loggar in till bank.	IP
25	FL	Jag tänker på det som blivit lyft med GDPR, att man måste ha ett syfte med den data som samlas in. Säg att du har ett system som samlar in data från en kund, måste du kunna påvisa syfte för vad du ska använda den datan till. Är det något ni fått jobba med?	
26	R4	Jag har jobbat med Vårdtjänsten och Banken, båda dessa kunder får inte samla in data om det inte är kunder till dem. Vårdtjänsten måste du anmäla dig till där, jag kan inte bara hitta på och lägga in något	SR,

		där. Samma sak gäller Banken, du måste själv skriva in informationen och signera, annars får man inte in något. När jag säger Banken är det inte bara Sverige utan det är hela Europa, jag är inte ansvarig för Sverige utan för hela Europa, till Sverige är det helt annat. Men vi samlar inte information och vi måste ta bort extra, typ det jag sade med graviditetsnyheterna. Två veckor efter barnet fötts måste mailadressen bort, även i loggen och alla ställen. Banken har egna regler.	
27	FL	Sen är det sånt med data minimization, att du inte samlar in och behåller data du inte behöver.	
28	R4	Nej absolut de gör de inte, eftersom det är en extra kostnad.	SR
29	FL	Är det något du har märkt att man jobbat mer med eller var det samma innan?	
30	R4	Grejen är att ta bort gammal data är inte så enkelt heller. Det finns kunder som låtit det ligga kvar eftersom de inte vill ta kostnaden för att ta bort den. De vet inte hur viktig den gamla datan är, är den viktig eller inte? Vilken ska de behålla? Så de har inte lagt någon röd tid. Men efter GDPR kunden tvungen, även små företag, att lägga en röd tid. Jag är säker på att många säger att de följer GDPRS regler men jag är säker på att de inte gör det. GDPR går även in på loggarna, så jag tror inte att det är många som kollar loggarna och vill ta bort från dem. Det är ett riktigt stort jobb. Även t.ex. Banken visste inte det, vi har kundinformation i loggarna för att när du provar att logga in, på låg nivå kollar de att den personen har provat att logga in. Så efter fem år efter att du slutar måste den loggen också bort. Om du inte har en röd tid där så...	SP, SR
31	FL	Är det något du har varit tvungen att lägga fram lösningar för?	
32	R4	Ja precis, för DK, Finland och Norge har jag tvingat kunden att göra den lösningen. Det är inte att kunden inte vill göra det, men när det är storföretag måste någon ta ansvaret för att ta bort det. För att kunden måste prata med advokater och sånt. Det är inte så enkelt som man tror “okej det är extra information vi tar bort den”. När det blir en stor firma är varje kund viktig och du kan inte bara ta bort den. Jag har tvingat dem att om de inte kommer använda den måste de ta bort den och tillslut godkände de att ta bort det. Man tänker inte heller på att skrivarna som finns på företagen håller kundinformation, hela tiden när man skriver ut skickar man från sitt AD-konto och det sparas där vem som har skickat. Jag har varit på den nivån till kunderna, jag vet inte heller om O4 följer det men det hoppas jag men man vet aldrig, det är inte mitt jobb, vi har en AT-avdelning. Jag är ansvarig för en annan firma.	SP, SR, AF
33	FL	Du pratade om right to be forgotten, har ni jobbat något med att utveckla lösningar mot slutkunden så att de själva kan t.ex. begära ut data?	

34	R4	Ja, det var med Vårdtjänsten vi gjorde ett system eftersom innan var det O4 som var ansvariga nu är det ett annat företag. Där kunde man själv skriva in sin mailadress och ta bort från t.ex. Nyhetsanmälningar. Sen var det ett annat system för att fråga anonyma frågor, när du är sjuk och vill fråga en läkare, gratis och anonymt. Men end-users tänker inte, det heter anonyma frågor men de kommer och säger "Hej jag heter Bertil och detta är mitt personnummer" men det är anonyma frågor. Vi skapade ett system där man kunde lägga in sin mailadress och systemet kommer ta mailadressen och varje vecka samla allt som vi fått och rensa bort.	SR
35	FL	Vi snackade om testning, men gör ni code review?	
36	R4	Ja men code review, jag tror inte att det gör mycket om du frågar om GDPR. Vi gör code review hela tiden när du utvecklar vanliga system, du måste ha det. Det är lätt när man skriver kod att du i ditt huvud tänker att allting är rätt men när jag kommer och ser att du kanske gjorde en metod public när den borde vara private istället för att du inte vill att en annan klass ska komma åt den. Det finns code review, men inte på grund av GDPR, det är en vanlig rutin att det hela tiden finns code review innan man checkar in sin kod.	RI, DS
37	EO	Men GDPR frågor löser man mer på arkitektnivå menar du? Är det för sent att lösa det vid en code review?	
38	R4	Du gör code review bara för att säkra att utvecklare har utvecklat på det sättet man tänkte. GDPR börjar helt och hållet från designen. Det är inte någon utvecklare, vi är en stor firma, utvecklare tar inte den rollen som kan tänka på GDPR. De får helt enkelt inte betalt för att tänka på GDPR.	R, SP
39	FL	Om vi ser till systemutvecklingsprocessen, vi använder SDLC, vi har kravställning, design och kodning/testning, var skulle du säga att man bryr sig mest om privacyfrågor?	
40	R4	Det börjar absolut från första, kravställningen, sen när du gör designen så kan du upptäcka att det finns saker de inte tänkt på. Även när du kommer till utvecklingen, för att det finns hela tiden en tech lead, där kan man upptäcka att man har privacy issues och så får det gå tillbaka till designen. De kommer inte lösa det på development, det måste gå till designern och designern gör lite ändringsförslag, typ 2-3 eller vad som är möjligt. Sedan går det till kravställning och de säger "Okej, här måste vi byta kraven". Det måste hela tiden gå från första.	SP
41	FL	Så den går uppifrån och ner och sen tillbaks upp om den hittar något?	
42	R4	Ja, om vi ser om det är här det följer… Det kommer inte följa regler eller så, då den måste gå hela vägen upp. Annars vi kommer leverera någonting där kraven säger något helt annat.	SP

43	FL	Vilken utvecklingsmetodologi kör ni, är det agilt eller?	
44	R4	Det beror på. Scrum, Kanban, det beror på vilken firma man jobbar med. Innan hade vi spring planering typ i kanban, nu har vi bytt till agilt, det är nytt hela tiden och ibland har vi jobbat med waterfall. Det är varje… Om du frågar för O4 så; O4 jobbar med allt, det är vad kunden säger, men agilt är det nyaste som de vill ha. Kunden också kan inte varje månad, typ varje vecka göra en release. Även Apple de gör inte det men de kallar sig agila. Men agilt är hela tiden: "Okej, den koppen är full - gå till produktion". Man måste planera, vi är agila så mycket som vi kan., men det är helt kunden som lägger de kraven; hur man måste jobba.	
45	EO	Skulle du säga att krav på digital integritet hämmar innovationen inom systemutveckling? Att begränsar innovationen?	
46	R4	Eh, ja, du kan se här: alla mail jag får de är GDPR-relaterade, det är så. Det är utvecklare som har checkat in koden så jag måste reviewa innan vi går vidare. Klart, det är de som betalar för det, de lägger begränsningarna, men ibland vi har kunder som säger, det är typ Vårdtjänsten; "Lägg allting hos oss, ni är ansvarigt för, och jag väntar mig ni levererar topp". Men det är klart att den begränsningen det är hela tiden det beror på hur mycket de vill satsa. När du jobbar hos bank, allting är stängt, de jobbar med legacysystem som är utevecklat i 90-talet så man kan inte bli så öppet som möjligt. Vi kan inte använda ny teknologi som vi vill, det är hela tiden begränsat men andra kunder de är helt öppna.	DI, AF, SP
47	FL	Ser du några… Eller det har du ju lite sagt och nämnt, men ser du några förändringar med ditt eget arbete med integritet i systemen sedan GDPR?	
48	R4	Det är klart, nu det är GDPR när det… Förra maj det var sån stor grej, det var alla prata om GDPR, även de höga cheferna de förstod ingenting. De kom och bara frågade: "Eh, vi följer GDPR-regler och så?" Det är bara för att najs to say, vi hade mycket tryck på det. Fortfarande vi har men det är inte som innan, jag tror efter 3-4 år det kommer bli skit samma. Men absolut, det är bra regel, jag såg innan många företag som har gjort det mycket pengar bara för att de sålde kunddatabaser men nu det finns tryck på GDPR. Men jag väntar mig att det trycket kommer… (avta, reds anm)	SP, DI
49	FL	Men tror du att den kommer.. Eller känner du att i era systemutveclingsprocesser, har det påverkat mycket där? Har det blivit några nya aktiviteter i utvecklingsprocesserna?	
50	R4	Det är klart, ja. Innan det var inte en huvudrequirement att vi följer den, innan det var bara - det finns ingenting och nu det är en requirement så man… Även kunden måste tänka: "nu kommer det (GDPR, reds anm) till oss" och om de har inte tänkt på det så måste vi flagga: okej här, hur tänkte ni här?"	SP

51	FL	Händer det ofta att ni behöver flagga för det?	
52	R4	Ja, hela tiden. Det är hela tiden. Det är första gången det är cheferna (som säger, reds anm): "okej, våra system var fett nice" men även kunden bryr sig inte om security. De säger att det spelar ingen roll men vi säger att det kan inte… "Ja, men vad får jag tillbaka? Det är security, ja men men varför?" Det är så.	SP, DI
53	FL	"Det kostar pengar, men varför ska jag göra det?"	
54	R4	Med security måste man hela tiden utveckla vidare, och där har vi problem med kunderna, nästan alla. Nästan ingen vill satsa på security.	DI, AF
55	FL	Och det är för att det kostar pengar?	
56	R4	Det kostar pengar. If it's working why change it? Det är en gång man kan hacka den och efter det… Men jag har inte träffat någon kund som… Det är nice to see men när det kommer ett kostandsförslag så säger de "nja, kanske, vi får se".	AF, DI
57	EO	Men höll ni på och flaggade mycket för sådana här problem och potentiella risker även innan GDPR?	
58	R4	Ja, ja, för att det är en risk. Vi vill inte utveckla någonting och se på nyheterna att någon har hackat det. Så det är klart, vi har flaggat hela tiden, men vad är skillnaden? Innan har kunden inte reagerat alls, nu börjar de reagera eftersom innan har de reagerat när vi ser: "okej om kundinformationen går ut kommer det påverka ditt jobb". Men nu finns det en regel också, så nyheterna kommer skriva om det händer något med stora kunder. Ibland har jag också hört att de som anmäler till GDPR inte bara är privatpersoner, det är konkurrenter också. Det är hela tiden så att kunden måste tänka på GDPR.	R, AF, DI, SP
59	Fl	Händer det att ni säger nej till projekt för att de inte…?	
60	R4	Jag är inte säljare, så jag kan inte svara på det, hehe. När det kommer till mig är det redan satt och påskrivet. Jag kan hela tiden säga till min chef att jag inte vill jobba med den kunden pga det och det och det men jag har inte rätten att neka hela O4.	SP
61	FL	Nu ska vi se om vi har några frågor kvar, det har vi nog inte egentligen. Hur var det med era policys och dokument? Har ni några sådana som är specifika för hur man ska arbeta med privacy?	
62	R4	Ja absolut. Innan jag började på Banken hade jag en kurs under en månad. Allt, allt från hur jag dricker vatten när jag pratar med dig till var datorn ska ligga, vilken nivå av encrypting. Grejen är det, vilken kund… Men det finns absolut. Typ vårt utvecklingsrum ligger där, där har vi ett vanligt utvecklingsrum och där finns kod och allting. Man får inte lägga typ sin dator olåst där, även om vissa datorer, typ min kan jag göra det med om jag vill. Efter 2 minuter kommer det en	U, IP, DS

		screensaver som man inte får ändra, det är O4s policy, så det är absolut så. O4 är mycket, mycket, privacy är först för oss. Vi får inte göra mycket heller, typ jag kan inte bjuda kunder på någonting, det är policys och det finns mycket sånt hos O4 p g a att man är en stor firma.	
63	EO	Ja, för det var också något jag tänkte på som du sade. Just det här med att även om… För när kunden har köpt in systemet och när ni har utvecklat färdigt ett system så är det ju kunden som är ansvarig för alla privacy issues. För vi har pratat med andra konsulter som har sagt att det är upp till kunden, men just det här du sade att kommer det ut att det är någon som har hackat systemet så reflekterar ju det dåligt på er.	
64	R4	Ja, det är skillnaden mellan små och stora kunder. Vi har aldrig utvecklat något och bara lämnat det vidare för det finns vårat namn bakom. Det finns inget system man kan utveckla som är buggfritt till hundra procent. För att Chrome uppdater sig varje gång. Alla system som är berörda kommer behöva utvecklas då. Så om jag säger: "Okej, det här systemet det kommer fungera till hundra procent i ett år", det tror jag inte, för du har använt libraries och du har mycket beroende av andra system. Om de har uppdaterat sig så måste du också uppdatera dig. Så vi lämnar aldrig, och när en annan kund tar över vår utveckling så måste vi ha typ en knowledge transfer under en period för att berätta hur det har fungerat och så.	AF, RI
65	EO	Du menar om ni anställer en underleverantör?	
66	FL	Nej, om någon annan tar över projektet.	
67	R4	Ja, precis så, om någon annan tar över något. För ibland säger de "Okej, O4 de är bäst på att utveckla någonting men de är inte billigast för att underhålla det, vi har en annan firma som tar över den." Absolut, men vi måste ha en knowledge transfer, vi accepterar inte bara att någon tar vårt system. Kunden bestämmer, det är deras kod och deras ansvar, men från början när vi skriver kontraktet så säger vi att vi måste ha knowledge trasnfer. Det är inte bara att vi lägger över det och bara: "you're on your own", det är aldrig så.	AF, SP
68	FL	Nej, det är spännande, för det skiljer sig mot andra vi har frågat. För de säger såhär: "Det är bara upp till kunden, vi skriver det och lämnar det där" och sen så...	
69	R4	Nej, så är det absolut inte (för oss) Vi vill inte att vi utvecklar någonting och på slutet så kommer du höra om oss på typ nyheterna och du läser om oss, så är det absolut inte. För att vi har stora kunder (räknar upp ett antal stora kunder), vi får aldrig små kunder. Jag kan inte säga att det beror på säljarna som säljer projektet, men de (de små kunderna, reds anm) är inte intressanta för oss. Men när man fokuserar på stora kunder så är det hela tiden… Det är eftersom vi fokuserar på stora kunder som vi kan satsa på det vi gör.	AF

70	FL	Ja, för det låter som ni är mer engagerade...	
71	EO	...och tar ett större ansvar än många andra konsultbolag	
72	R4	Nej, nej, vi tar ansvar, och vi tar ansvar på riktigt. När banken går ner eller något system går ner, hela tiden… och hela tiden finns det ett team som reviewar vår kod och vår utveckling. Typ om vi gör en deployment till produktion så har vi ett annat team som går till systemet, vi vet aldrig vem från O4 det är, de kanske sitter i Sverige, kanske i Indien, som folk sitter och gör olika test. Performing tests, hacking tests och så och efter en månad eller två veckor så får vi ett resultat. Om det resultatet är dåligt så måste vi agera också, det är viktigt.	AF, RI
73	EO	Just för att du inte ska kunna påverka, om du känner kollegorna som jobbar med den testningen, att du inte ska kunna påverka dem eller så?	
74	R4	Ja, ja, det är klart, för testarna går hela tiden till utvecklarna. Jag testar på det sättet om det här inte lyckas. Och plus om jag ser ett UAT, acceptanstest, så är det kunden som testar och inte våra testare, de måste ha sånt. Ett testteam som testar så vi vet att vi har levererat vad kraven säger.	RI
75	FL	Spännande. Alltså vi har inte några direkta frågor men bara så här allmänt; vad betyder privacy och integritet för dig?	
76	R4	Ja, det är jag. Om någon tar min privacy och allting så... Man kan göra vad du vill, typ en sådan ID thief eller någonting. Men i Sverige är vi riktigt bra, även om alla system är öppna så har vi samtidigt en riktigt bra privacynivå för att vi kollar, typ t ex i England, det är ett exempel. De har inga personnummer, det är helt sjukt. Så om vi ser två personer och jag vet inte, jag heter Bert Bertilsson, och om jag har ett barn och han heter Bert så bor vi båda på samma adress och vi har samma namn, han heter också Bert Bertilsson. Om jag är bra, och han är mycket dålig, eller tvärt om, så kan han inte få lån - vem är bra? Där är det lätt att man gör en identity theft, på grund av att det går på adressen och ditt namn, det finns ingen riktig person. Men här har vi personnummer och hela tiden behöver man visa sånt. Med Mobilt BankID, det är digital privacy. Den som utveckar Mobilt BankID - banken måste tro på dem och om någon kan hacka den så.... Men för mig är det stor grej, jag vet inte, jag har inte brytt mig mycket om jag inte är på sociala medier och så och på samma sätt tror jag allting måste bli öppet. Folk måste veta vem är jag, de kan hitta mig och läsa mycket, jag är helt öppen med det. Men samtidigt vill jag inte att de vet vilken sjukdom jag har, det är min rätt. Om det är min rätt att jag håller det hemligt så vill jag göra det starkt, jag vill inte bli öppen med det och jag kommer bli mycket arg om någon har tagit ut den (informationen).	DI
77	FL	Ja, alltså om de tar din information, om dig.	

78	R4	Ja, de får inte, så den firman som har tagit ansvaret måste hålla det. Ja, privacy och man blir öppen… Man måste, ja...	DI
79	FL	Man måste avväga det.	
80	EO	Ja, det är en balansgång liksom.	
81	R4	Ja, det är en balansgång, hur mycket är viktigt. Folk säger "Nej, jag lägger inte upp någon bild på mig." Det är din rätt, typ din rätt att du inte lägger någon… Men på andra sätt, Skatteverket är öppet, de skickar din deklaration, din adress och vem som bor med dig, hur många hundar du har och allting, det finns. Du kan, jag kan bara ringa Skatteverket och fråga.	DI
82	EO	Ja, jag förstår vad du menar. Vi har väl inga mer konkreta frågor, känner du att det är något vi har missat?	
83	R4	Jag vet inte vad ni skriver om, men privacy är inte bara GDPR, det är bara det vi ser. Det finns många firmor som upp till nu har de inte skapat… När du surfar till deras sida har de inte HTTPS, så man börjar… Jag har sagt till någon firma att jag vill inte se någon webbsida där de säger "Vi håller på GDPR" och så har de inte HTTPS, så hur håller de? Om jag loggar in så kan jag hacka deras system på… Jag tror att det är en lång resa, det är inte alla som har… De säger att de har, det är solklart många som inte har gjort det, det är bara på papperna och så det är snyggt. Det är som miljö typ; "vi sorterar och så", på riktigt sorterar de ingenting. Även O4 är hur starka som helst på det, vi måste sortera och så, allting när vi kastar något vi inte får. Om du går till kitchen area, allting måste bli sorterat så jag tror om ni kommer skriva om privacy så är GDPR en stor punkt för det är nytt, men det finns mycket under. Typ hur man kan hålla sin privacy även om vi är i ett land där allting är öppet, nästan allting är öppet i detta landet. Så kan vi hålla oss på den privacy som redan… Typ min journal och sånt, vill jag inte ska komma ut, hur starka vi är att vi håller det i Sverige. Jag vet inte vad ni skriver om så… Det är bra att ni skriver om GDPR för det är nytt.	DI, DS
84	FL	Hehe, ja, vi har det som en… Eftersom folk har börjat tänka på det mer i och med GDPR, även om man tänkte på privacyfrågor innan. Men vi tänker på mycket så här personlig integritet, ja men säg att jag använder Facebook och de samlar in data om mig - vad använder de den datan till? Sådana frågor.	
85	EO	Så GDPR blir ju mer ett exempel eller ett fall som har lyft upp det här med privacy på agendan så att vi kan titta på hur det såg ut innan och hur, om det har förändrats någonting efter GDPR, när det kommer till privacy.	
86	R4	Nu, med privacy, är det helt sjukt även om jag tror att det måste finnas starkare lagar p g a att jag är lite sån… Ibland tror jag att mobilen lyssnar på mig, faktiskt, för det har hänt mig att jag har pratat om	DI

		någon bil eller jag vet inte, och sedan har jag öppnat Facebook och så har den bilen kommit upp. Det var kanske coincidence, men...	
87	EO	Nej, jag har upplevt precis samma sak.	
88	R4	Det är därför redan när det är ett viktigt möte så provar jag att lägga min mobil ute för att man vet om det är private sector… Ibland säger man: "Okej, varför vill du hålla din privacy, har du något du vill gömma?" Nej, det är inte så, jag vill inte, men på samma sätt vill jag inte typ...	DI
89	FL	Bli trackad?	
90	R4	Ja, trackad eller någonting. Typ när jag startar min bil så vet min mobil redan var jag ska köra, den vet redan det och det är helt sjukt	DI
91	EO	Ja, det är obehagligt, jag håller med. Man behöver ju inte ha någonting att gömma för att vilja behålla sin personliga integritet.	
92	R4	Jag tror att även om det är bra att den är intelligent och sånt så måste man ha en knapp för att säga: "Jag vill inte ha det" så det är bara att stänga av - det är GDPR. Det är början av den. Jag vill inte att Google ser vad jag letar efter, typ om jag letar efter en studsmatta eller någonting så ser jag hela tiden… Även ibland så får jag ett mail med reklam på saker jag har sökt på Google. Cookies, det är en sak man måste, när du surfar använder cookies för mycket grejer och jag tror man måste ha rätten att stänga dem. Om du går till polismyndigheten eller någon så säger de att: "Vi använder cookies", för det är en regel i EU att man måste sätta en sådan banner. Men det finns ingen regel som säger om man inte vill att "Jag accepterar inte det" men om du inte accepterar det måste du lämna sidan men vad de inte säger är att de redan har sparat din personliga information. Så vad var lösningen för alla hemsidor? De har bara lagt till en banner, inte tagit bort den IP-adressen som du har surfat från.	DI
93	EO	Nej, det är verkligen bara en nödlösning.	
94	FL	Men jag tänkte bara snabbt, alltså i era projekt verkar det ju inte handla så mycket om tracking, personlig data och så utan det är mer security?	
95	R4	Ja, för vi har kunder som bryr sig om sina egna kunders och users, de bryr sig inte om typ andra kunder som andra har. Så huvudansvaret är att vi håller våra kunder och håller deras rättigheter, speciellt när det gällde Vårdtjänsten. Jag förstår inte hur t ex läckan hos Vårdtjänsten, jag köper inte vad de säger på nyheterna. "Det är en NAS-drive", och så. Om det företaget är på den nivån så vet jag inte hur de har skrivit kontrakt med dem, myndigheten, hur de har har skrivit kontrakt med dem. Och jag tar ansvar för vad jag säger nu, det är på riktigt, om de är på den nivån att de lägger det på en hårddisk eller NAS-disk, det är…	DI, DS, AF

96	EO	Helt öppet, ja, det är faktiskt helt galet.	
97	R4	För att om du är en så stor firma och sparar alla information på en NAS-disk, det är inte på någon riktig server. I Vårdtjänsten hade vi en server som kunde klara en atombomb, på riktigt. Det är hur man tänker för man vet inte, om någon kanske attackerar oss så måste man ha en kanal som kan ge information i en sådan situation. Och de håller det på en NAS-disk? Ja, det är oseriöst. Faktiskt, jag köper inte vad de säger, om de på riktigt är på den nivån, jag vet inte...	DS
98	EO	Spännande. Tack så jättemycket, verkligen, tack för att du har tagit dig tiden!	

Referenser

Birnhack, M., Toch, E., & Hadar, I. (2014). Privacy mindset, technological mindset. *Jurimetrics*, *55*, 55. Hämtad 20 Maj 2019 från: https://link.springer.com/article/10.1007/s10664-017-9517-1

Cavoukian, A. (2011). *Privacy by Design, The 7 Foundational Principles*. Hämtad 25 April 2019 från: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7foundprinciples.pdf

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society*, 3(2), 405-413. Hämtad 15 Maj 2019 från: https://link.springer.com/article/10.1007/s12394-010-0053-z

Chen, S. and Williams, M.A. (2013). *Grounding Privacy-by-Design for Information Systems* Pacific Asia Conference on Information Systems (PACIS) 2013 Proceedings. 107. Hämtad 10 Maj 2019 från: http://aisel.aisnet.org/pacis2013/107

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). *Privacy and data protection by design-from policy to engineering*. Aten: European Union Agency for Network and Information Security. Hämtad 20 maj 2019 från: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Datainspektionen. (2019a) *Inbyggt dataskydd och dataskydd som standard*. Hämtad 20 maj 2019 från: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/inbyggt-dataskydd-och-dataskydd-som-standard/

Datainspektionen. (2019b) *Dataskydssförordningen GDPR*. Hämtad 20 maj från: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/

Datatilsynet (2017). *Guide - Software development with Data Protection by Design and by Default*. Hämtad 20 maj 2019 från: https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/

Davies, S. (2010).*Why Privacy by Design is the next crucial step for privacy protection*. London: Initiative for a Competitive Online Marketplace (ICOMP). Hämtad 20 maj 2019 från: https://pdfs.semanticscholar.org/7ffc/32552027757110ad60b3ae701148b702f706.pdf

Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 04.05.2016, s. 1–88). Hämtad 20 maj 2019 från: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52012PC0011

Förslag till Europaparlamentets och Rådets förordning COM (2017) 10 final av den 10 januari 2017 om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation). Hämtad 20 maj 2019 från: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52017PC0010

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

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*, *23*(1), 259-289.

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

Insight Intelligence. (2018). *Delade Meningar - Svenska folkets attityder till digital integritet 2019*. Hämtad 20 maj 2019 från: http://www.insightintelligence.se/wp-content/uploads/2019/03/deladeMeningar2019_Web_1-6A.pdf

Jacobsen, D. I., & Sandin, G. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*. Lund: Studentlitteratur.

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: the PriS method. *Requirements Engineering*, *13*(3), 241-255.

Kurtz, C., & Semmann, M. (2018). Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. *Association for Information Systems*

Lindström, K. (2018). I dag smäller det – GDPR börjar gälla. Så vad händer nu?. *Computer Sweden*. 2018-05-25. Hämtad 29 april 2019 från: https://computersweden.idg.se/2.2683/1.703090/gdpr

Microsoft. (2012). Microsoft Security Development Lifecycle (SDL) Process Guidance - Version 5.2. *Microsoft.* 2016-12-10. Hämtad 20 maj 2019 från: https://www.microsoft.com/en-us/download/details.aspx?id=29884

Oates, B. J. (2005). *Researching information systems and computing*. London: Sage Publications Inc.

Proposal for a Regulation of the European Parliament and of the Council COM (2017) 10 final av den 10 januari 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). EGT L 201, 31.7.2002, s. 37–47. Hämtad 20 maj 2019 från: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010

Proposal for a Regulation of the European Parliament and of the Council COM (2012) 11 final av den 25 januari 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Hämtad 20 maj 2019 från: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011

Sheth, S., Kaiser, G., & Maalej, W. (2014, May). Us and them: a study of privacy requirements across North America, Asia, and Europe. In *Proceedings of the 36th International Conference on Software Engineering* (pp. 859-870). ACM.

Svenska Akademiens ordbok. (1933). *Integritet*. Hämtad 2019-05-20 från https://www.saob.se/artikel/?unik=I_0881-0080.8813

Valacich, J. S., George, J. F. (2016). *Modern Systems Analysis and Design*. 8th edition. Boston: Pearson Education Limited.

van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2012, October). Designing privacy-by-design. In *Annual Privacy Forum* (pp. 55-72). Springer, Berlin, Heidelberg.