LUNDS UNIVERSITET
Ekonomihögskolan
Institutionen för informatik

Privacy by Design i svenskt näringsliv

En empirisk studie på integritet & Privacy by Design i systemutveckling

Kandidatuppsats 15hp, kurs SYSK16 i Informatik

Författare: David Nilsson
Petter Andersson

Handledare: Odd Steen

Rättande lärare: Benjamin Weaver
Umberto Fiaccadori

Förord

Vi vill börja med att tacka vår handledare, Odd Steen, som bidragit med insiktsfull kritik och viktiga åsikter genom hela uppsatsprocessen. Vi vill också rikta ett tack till personerna som ställde upp på intervju och bidrog till vårt empiriska resultat.

19 maj 2021

David Nilsson & Petter Andersson

Privacy by Design i svenskt näringsliv: En empirisk studie på integritet & Privacy by Design i systemutveckling

ENGELSK TITEL: Privacy by Design in Swedish business: An empirical study on integrity & Privacy by Design in system development

FÖRFATTARE: David Nilsson, Petter Andersson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Christina Keller, Professor

FRAMLAGD: maj, 2021

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 85

NYCKELORD: Privacy by Design, Privacy, Integritet, GDPR, Dataskyddrätt

SAMMANFATTNING (MAX. 200 ORD):
Integritet eller ”privacy” är ett komplext begrepp och har med uppkomsten av ansatser och regelverk såsom Fair Information Practices (FIP:s), Privacy by Design (PbD) och GDPR blivit alltmer omtalat. PbD som ansats förespråkar ett organisationsomspännande perspektiv på integritet och ansatsen har kritiserats för att bland annat vara vag och svår att implementera i praktiken. I tidigare studier har stort fokus legat på utvecklarna och deras svårigheter med PbD. Syftet med denna uppsats är därför att undersöka och beskriva hur personer med ett formellt ledarskap och deras organisationer arbetar med integritetsfrågor i förhållande till ansatsen. Uppsatsens empiriska resultat består av tre intervjuer med personer som besitter ett formellt ledarskap. Resultatet av vår studie pekar på att organisationerna inte följer ansatsen Privacy by Design vid hantering av integritetsfrågor. Flera av PbD:s principer kan däremot spåras till aktiviteter som organisationerna utför. Samtliga företag arbetar aktivt med integritet i utvecklingen av system men det framgår att utgångspunkten till integritet ser olika ut hos organisationerna. En organisation säger exempelvis att affären kommer först och en annan menar att integritet styr deras tekniska innovation.

Innehåll

1 Introduktion 2
1.1 Bakgrund 2
1.2 Problemområde 3
1.3 Forskningsfråga 4
1.4 Syfte 4
1.5 Avgränsningar 4
2 Tidigare forskning inom Privacy, PbD & Europeisk dataskyddsrätt 6
2.1 Privacy 6
2.2 Integritet vs Säkerhet 7
2.3 Fair Information Practices 7
2.4 Privacy by Design 8
2.4.1 De sju fundamentala principerna 8
2.4.2 Utmaningar med Privacy by Design 10
2.4.3 Möjligheter med Privacy by Design 11
2.4.4 Lösningar och andra tillvägagångssätt 12
2.5 General Data Protection Regulation 13
2.5.1 Skäl 78 & Artikel 25 13
2.5.2 Artikel 5 & 6 13
2.5.3 Avsnitt 2 & 3 14
2.6 Litteratursammanfattning 15
3 Tillvägagångssätt 17
3.1 Litteraturgenomgång 17
3.2 Metodval 17
3.3 Urval 18
3.3.1 Val av organisation 18
3.3.2 Val av intervjuperson 19
3.4 Intervju 20
3.4.1 Pilotintervju 20
3.4.2 Intervjuguide 21
3.5 Bearbetning av empiri 24
3.5.1 Transkribering och kodning 24
3.6 Undersökningskvalitet 25

3.6.1 Reliabilitet 25
3.6.2 Validitet 26
3.7 Etik 27
4 Empiriska resultat 29
4.1 Begreppet "Privacy" 29
4.2 Proactive not Reactive; Preventive not Remedial 30
4.3 Privacy Embedded into Design 30
4.4 Full Functionality – Positive-Sum, not Zero-Sum 31
4.5 End-to-End Security – Lifecycle Protection 32
4.6 Utmaningar 33
4.7 Möjligheter/motivering 34
4.8 Lösningar & andra tillvägagångssätt 35
5 Diskussion 36
5.1 Synen på begreppet "Privacy" 36
5.1.1 Privacy 36
5.1.2 Privacy vs Security 36
5.2 Proactive not Reactive; Preventive not Remedial 37
5.3 Privacy Embedded into Design 38
5.4 Full Functionality – Positive-Sum, not Zero-Sum 38
5.5 End-to-End Security – Lifecycle Protection 39
5.6 Utmaningar 40
5.7 Möjligheter/motivering 40
5.8 Lösningar & andra tillvägagångssätt 41
6 Slutsats 42
Appendix A 44
Appendix B 45
Appendix C 57
Appendix D 67
Referenser 75

Tabeller

Tabell 1: Karaktären hos PbDs principer 15
Tabell 2: Utmaningar & möjligheter 16
Tabell 3: Intervjusubjekt & Organisationer 19
Tabell 4: Övergripande intervjuguide 22
Tabell 5: Intervjuguide 23
Tabell 6: Kodningsmall 25
Tabell 7: Relaterad princip 1 44
Tabell 8: Relaterad princip 2 44
Tabell 9: Relaterad princip 3 44

Definitioner

Definitioner och förtydligande inom ramen för denna uppsats.

Begrepp	**Definition**
Ledare	Exempel på organisatoriska arbetsroller: projektledare, avdelningschef, landschef, CDO, CIO, CTO.
Ledarskap	”Som chef måste du hantera relationer, förhålla dig till ramar, leverera resultat och leda verksamheten i en riktning.” och ”Ledarskap är något som sker i relation till andra, och är ett verktyg för att nå mål och lösa uppgifter – att skapa resultat. Ledarskapet kräver också ramar och strukturer i den organisation eller kontext du är verksam.” (Ledarna.se, n.d.)
Privacy	“Privacy” på engelska är ett komplext begrepp med olika definitioner som omfattar olika betydelser (Kroener & Wright, 2014). Än mer komplext blir det då ordet ”privacy” har olika översättningar till det svenska språket. Begreppet, som är taget ur engelsk litteratur kommer inom ramen för denna uppsats att benämnas som ”integritet”.
Integritet	I det svenska språket har ordet integritet flera betydelser. Talar man om integritet i samband med utveckling av it-artefakter mot privatkonsumenter, så syftar det vanligtvis på personlig integritet. När vi i denna uppsats använder ordet integritet är det därmed den personliga integriteten vi syftar på.
Personuppgifter	”Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet” (EU, 2016, p.33).
Registrerad	”en identifierad eller identifierbar fysisk person” (EU, 2016, p.33).

1 Introduktion

1.1 Bakgrund

Personuppgifter och användardata är idag en produkt som fått ett allt större kommersiellt värde samtidigt som oron att dela med sig av personuppgifter digitalt ökat (Insight Intelligence, 2021). I en årlig studie från Insight Intelligence (2021) i samarbete med Karlstad universitet, Arbetsförmedlingen, Skatteverket och IAB Sverige syns det tydligt att svenska folket är oroliga för att den personliga information som de delat med sig av digitalt, används för syften som de inte är bekväma med (44% år 2021). Siffran har dessutom stigit stadigt från 2015 (22%) fram till 2020 (49%) och först i år (2021) har siffran sjunkit med 5 procentenheter (Insight Intelligence, 2021).

Begreppet digital integritet har länge varit på tapeten och har tagit fart i samband med bland annat dataläckor och riktade påverkanskampanjer (Insight Intelligence, 2021). 2007 blev Europeiska unionens stadga om de grundläggande rättigheterna (EU, 2010/C 83/02), även kallad rättighetsstadgan, uppdaterad för att slutligen bli rättsligt bindande genom Lissabonfördraget 2009. I artikel 8.1 i rättighetsstadgan kan vi utläsa följande;

> 1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne. 2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. 3. En oberoende myndighet ska kontrollera att dessa regler efterlevs (Europeiska Unionen, 2010/C 83/02, p.5).

För att vidare skydda fysiska personers fri- och rättigheter i samband med behandling av personuppgifter instiftades ”Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter”, även känd som General Data Protection Regulation eller GDPR. GDPR trädde i kraft 25 maj 2018 och höjde ribban gällande digital integritet. Företag tvingades ändra och granska sina system för att säkerställa att de följde det nya direktivet. För många bolag var detta en stor omställning. Även om företagens affärsidé inte direkt kretsade kring behandling av personuppgifter så behandlar de ofta personuppgifter i system som exempelvis CRM-system, sälj- och marknadsföringssystem samt HR- och lönesystem.

Trots stor uppståndelse vid tillämpningen av GDPR 2018, har den upplevda tryggheten till följd av den inte nödvändigtvis ökat. Insight Intelligence (2021) påpekar att 45% av studiens respondenter tycker att lagar och regler har störst påverkan på känslan av trygghet i relation till personuppgiftshantering. Samtidigt tyckte endast 14% att de kände sig mer trygga som en direkt följd av GDPR under mätningen 2020 (Insight Intelligence, 2021). Statistiken talar för att Insight Intelligence (2021) har rätt när de säger ” … att det främst är idén om lagar och regler som skapar trygghet snarare än enskilda lagar och regler i praktiken” (Insight

Intelligence, 2021, p.7).

En omtalad del av GDPR är artikel 25 och skäl 78 i ingressen som handlar om inbyggt dataskydd och dataskydd som standard ((EU) 2016/679 artikel 25, skäl 78). Inbyggt dataskydd och dataskydd som standard bygger på samma principer och delar många likheter med ansatsen Privacy by Design (European Data Protection Supervisor, 2018). Privacy by Design har sitt ursprung i ett samarbete mellan de nederländska och kanadensiska dataskyddsmyndigheterna. Samarbetet ledde 1995 till en rapport om PET:s (Privacy enhancement technology) som Dr Ann Cavoukian senare vidareutvecklade till vad som idag är känt som Privacy By Design (Bu, Wang, Jiang & Liang, 2020; van Lieshout, Kool, van Schoonhoven & de Jonge, 2011).

1.2 Problemområdes

Privacy by Design (PbD) är en ansats till integritetsarbete som betonar vikten av proaktivt skydd och innebär att integritetsskydd ska beaktas under hela produktens livscykel (Cavoukian, 2009; Hustinx, 2010). 2008 presenterade Cavoukian sju grundläggande principer för PbD med syfte att fungera som ett referensramverk för att förstå och tillämpa PbD (Cavoukian, 2009). Cavoukian (2009) uttrycker att integritet måste införlivas i nätverksanslutna datorsystem och teknik som standard och behöver således bli en integrerad del av organisationers prioriteringar, projektmål, designprocesser och planeringsverksamhet.

> Privacy must be embedded into every standard, protocol and process that touches our lives (Cavoukian, 2009, p.1-2).

Filosofin och de områden som de sju principerna uttrycker i referensramverket kan enligt Cavoukian (2009) tillämpas på specifik teknik, affärsverksamhet, fysiska arkitekturer och nätverksinfrastruktur men även hela informationsekosystem och styrningsmodeller. Det är tydligt att det enligt Cavoukian inte endast är utvecklare som behöver arbeta med PbD utan arbetet behöver snarare genomsyra hela organisationen.

PbD utvecklas hastigt och är idag ett erkänt begrepp inom informationsindustrin (Bu et al., 2020). Kritik har däremot riktats mot Cavoukians syn på integritet (Gürses, Troncoso & Diaz, 2015; van Rest, Boonstra, Everts, van Rijn & van Paassen, 2014) och anpassning och implementering av PbD hos organisationer har blivit en utmaning (Bu et al., 2020; Kroener & Wright, 2014). Termen PbD har utmålats för att vara för vag för att förstås av utvecklare (Bu et al., 2020) och även om PbD har införlivats av regelverk såsom GDPR så menar experter att det saknas tydliga instruktioner för hur implementeringen ska gå till (Spiekermann, 2012).

Efter att ha gått igenom tidigare studier (Bednar, Spiekermann & Langheinrich, 2019; Bu et al., 2020; Gürses, Troncoso & Diaz, 2011, 2015; Hadar, Hasson, Ayalon, Toch, Birnhack, Sherman & Balissa, 2018; Senarath & Arachchilage, 2018; van Lieshout et al., 2011) upptäckte vi att få empiriska studier har gjorts för att undersöka hur personer i en ledande roll arbetar med PbD. Detta kan bero på att mjukvaruutvecklare anses vara de direkta implementerarna av PbD (Bu et al., 2020). Stort fokus i tidigare empiriska studier har således legat på utvecklare och deras praktiska svårigheter med arbetet (Bednar, Spiekermann & Langheinrich, 2019; Bu et al., 2020; Hadar et al., 2018; Senarath & Arachchilage, 2018). Cavoukian har dock uttryckt att PbD bör ses som mer organisationsomspännande och experter

poängterar även att en av utmaningarna med PbD, är att få organisationers ledning med i integritetsstrategin (Spiekermann, 2012).

Av de anledningarna kommer denna uppsats fokusera på hur personer i en ledande roll och deras organisationer arbetar med integritet i förhållande till Privacy by Design. Beskrivningen av arbetet kommer sedan användas för att belysa eventuella möjligheter och utmaningar med ett organisationsomspännande integritetsarbete.

1.3 Forskningsfråga

När vi i uppsatsen nämner ledare eller personer i en ledande roll, syftar vi till personer som blivit tilldelade ett formellt ledarskap. Formellt ledarskap innebär att en person utsetts till ledare av till exempel styrelsen för ett företag. Ledarna kan befinna sig på vilken nivå som helst i en organisatoriskhierarki så länge de har blivit formellt tilldelade ett ansvar över en grupp människor. Exempel på sådana organisatoriska roller finner ni i listan över definitioner ovan. Med den definitionen av ledare som bakgrund och det problem som vi identifierat i föregående avsnitt landar vi i forskningsfrågan:

Hur förhåller sig integritetsarbetet hos personer i en ledande roll och deras organisationer till ansatsen Privacy by Design?

1.4 Syfte

Syftet med denna intervjustudie är att undersöka och beskriva hur personer i en ledande roll och deras organisationer arbetar med integritet i förhållande till ansatsen Privacy by Design. Vi kommer titta på vilka eventuella utmaningar och möjligheter som kan förekomma med detta arbete. Vi ämnar på så vis illustrera organisationers integritetsåtaganden och hur dessa förhåller sig till ansatsen PbD.

1.5 Avgränsningar

Under genomgång och läsning av tidigare litteratur på områdena Privacy by Design och dataskyddsrätt insåg vi att innebörden i tre av sju principer för PbD är väldigt lika några av de grundläggande krav som finns i Dataskyddsförordningens artiklar. En utgångspunkt som vi har haft under studien är att organisationerna som vi intervjuar följer lagar och regler. Vi avser inte att på något sätt bedöma verksamheters efterlevnad av olika legala krav som finns och vi fann det därför irrelevant för studien att undersöka hur dessa legala krav/principer uppfylls i de olika organisationer. Det är exempelvis inte relevant för denna studie om eller hur olika organisationer samlar in ett samtycke.

Principerna som inte kommer behandlas i denna uppsats är ”Privacy as the Default”, ”Visibility and Transparency” samt ”Respect for User Privacy”. Principerna och hur de korrelerar med Dataskyddsförordningen, återfinns i Appendix A, Tabell 7: **Relaterad princip 1**, Tabell 8: **Relaterad princip 2** och Tabell 9: **Relaterad princip 3**. De fyra principer vi kommer undersöka närmre finner ni i Tabell 5: **Intervjuguide**.

2 Tidigare forskning inom Privacy, PbD & Europeisk dataskyddsrätt

Detta kapitel är uppdelat enligt följande: inledningsvis kommer vi att behandla Privacy som begrepp och hur det förhåller sig till säkerhet. Vi går sedan vidare och presenterar Fair Information Practices samt Privacy by Design som ansats. Detta görs för att ge läsaren den information som krävs för att kunna förstå studiens ämnesområde och kommande referensram. I samband med Privacy by Design kommer vi även att visa på utmaningar och möjligheter med ansatsen samt andra tillvägagångssätt. Kapitlet avslutas med att redogöra för några av de delar av Dataskyddsförordningen som vi anser är relevanta för problemområdet.

2.1 Privacy

"Privacy" på engelska är ett komplext begrepp med olika definitioner som omfattar olika betydelser (Kroener & Wright, 2014). Traditionellt har betydelsen av "the right to privacy" argumenterats som en "right to be let alone". Flera möjliga lösningar för att skydda "privacy" har presenterats och sträcker sig från att uppmuntra organisationer till att anta rättvis informationspraxis (FIPs) till integritetsskydd online, sigill och certifikat. Begreppet bör däremot enligt Kroener och Wright (2014) betraktas i förhållande till lagstiftningsdefinitioner. Än mer komplext blir det eftersom olika översättningar av ordet "privacy" har presenterats till det svenska språket. Detta resulterar i att begreppet kan uppfattas som tvetydigt men även tolkas olika beroende på kontext och vem man frågar.

GDPR har varit restriktiva med att använda begreppet "privacy" och talar istället om rätten till skydd av personuppgifter "skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet" (EU, 2016, p.1). GDPR definierar vidare personuppgifter som "varje upplysning som avser en identifierad eller identifierbar fysisk person …" (EU, 2016, p.33).

En förekommande översättning av ordet privacy till svenskan är "integritet", vilken EU även valt att göra i Europaparlamentets och rådets direktiv 2002/58/EG direktiv om integritet och elektronisk kommunikation, som på engelska är Directive on privacy and electronic communications. I det svenska språket har ordet integritet även flera betydelser. När man talar om integritet i samband med utveckling av it-artefakter mot privatkonsumenter, så syftar det däremot vanligtvis på personlig integritet.

Personlig integritet definieras enligt NE såsom: "Rätt att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp (*personlig integritet*)" (Nationalencyklopedin, n.d.).

Det råder alltså oklarhet gällande hur begreppet privacy korrekt bör översättas till svenska men begreppet, som är taget ur engelsk litteratur, benämns inom ramen för denna uppsats som integritet.

2.2 Integritet vs Säkerhet

Spiekermann (2012) argumenterar för att en organisation behöver förstå vad de försöker skydda. Termerna privacy (integritet) och security (säkerhet) är ofta sammansmälta och Kroener och Wright (2014) säger att detta orsakar problem på två fronter. För det första, en avsaknad av att tydligt veta vad en organisation skyddar och med vilka medel. För det andra, integritet och säkerhet ställs ofta felaktigt mot varandra då det kan uppfattas som att vinna en är att förlora den andra. Att förlora personlig integritet leder inte nödvändigtvis till en vinst i fråga om säkerhet.

Ansatsen Security by Design bygger på att säkerhetskrav måste utformas i företagsarkitekturen från början (Kroener & Wright, 2014). Couvakian (2013 citerad i Kroener & Wright, 2014) föreslår att ansatserna Security by Design och Privacy by Design kan vara komplementära och konvergerande. Precis som att ansatsen Privacy by Design bygger på att integrera integritet i tekniken, så bygger Security by Design på att istället bädda in säkerhet i designen och skapandet av tekniken (Kroener & Wright, 2014).

Eftersom begreppen integritet och säkerhet ofta sammanfaller är det viktigt att skilja mellan dem i arbetet med Privacy by Design. Även om det finns lärdomar att ta från ansatsen Security by Design så bör Privacy by Design ses som en separat ansats. Att utforma säkerhet innebär alltså inte att integritet också har bäddats in vid utformningen av en ny teknik eller ett nytt system (Kroener & Wright, 2014).

2.3 Fair Information Practices

På 1980-talet presenterade Organization for Economic Co-operation and Development (OECD) åtta principer eller riktlinjer för att skydda integritet och dataflöden över landsgränser. Riktlinjerna refereras vanligtvis till som FIP:s eller ”Fair Information Practices” (Spiekermann & Cranor, 2009). Dessa riktlinjer kom över tiden att fungera som en grund för bland annat integritetslagstiftning i Europa (Spiekermann & Cranor, 2009) men också för integritetsansatser som Privacy by Design (Cavoukian, 2009). PbD:s principer kan anses omfatta och karaktäriseras av riktlinjerna i Fair Information Practices (Cavoukian, 2009). Riktlinjerna presenteras nedan med en kort beskrivning om vad de innebär.

Collection Limitation Principle
Begränsa insamling av data. Data ska samlas in lagligt och på ett rättvist sätt. Den registrerade ska vara medveten om datainsamlingen eller ha lämnat sitt samtycke till behandlingen (OECD, 2013).

Data Quality Principle
Insamlade personuppgifter ska vara relevanta för det insamlade syftet, korrekta och uppdaterade (OECD, 2013).

Purpose Specification Principle
Ändamålen för de insamlade personuppgifterna ska specificeras senast vid insamlingen av dem och användningen av dem ska vara begränsad till uppfyllandet av syftet för insamlingen eller andra syften som inte anses vara oförenliga med det ursprungliga ändamålet (OECD, 2013).

Use Limitation Principle
Insamlade personuppgifter ska inte avslöjas eller göras tillgängliga för andra syften än de ursprungliga, förutom om den registrerade ger sitt samtycke till detta eller att det krävs enligt lag (OECD, 2013).

Security Safeguards Principle
Personuppgifter ska skyddas med rimliga skyddsmekanismer mot bland annat förlust av data, otillåten tillgång, förstörelse och otillåten användning (OECD, 2013).

Openness Principle
Det bör finnas en policy om öppenhet i relation till behandlingen av personuppgifter. Det ska vara enkelt att få åtkomst till syftet för behandlingen samt att det ska vara enkelt att fastställa förekomsten och arten av personuppgifter som behandlas. Information om personuppgiftsansvarig eller underordnads identitet och huvudsakligt verksamhetsställe ska vara tillgänglig (OECD, 2013).

Individual Participation Principle
Registrerade ska ha rätten att få bekräftelse på om uppgifter relaterat till dem hanteras. De ska också få ta del av uppgifterna; inom en rimlig tid, utan eller inte överdriven kostnad, på ett resonabelt sätt och i en form som är för den registrerade hanterbar. Om en förfrågan för tillgång avslås ska den registrerade ha rätt att utmana ett sådant avslag och om utmaningen är framgångsrik, ha rätt att få uppgifterna borttagna, rättade, kompletterade eller ändrade (OECD, 2013).

Accountability Principle
Den personuppgiftsansvarige bör vara ansvarig för åtgärder som verkställer principerna ovan (OECD, 2013).

2.4 Privacy by Design

Som tidigare nämnt är Privacy by Design en ansats till integritet som förespråkar ett proaktivt skydd och ett holistiskt perspektiv (Cavoukian, 2009). Ansatsen togs fram av kommissionären för information och integritet i Ontario, Kanada, Ann Cavoukian. PbD består av sju principer som till viss del bygger på OECD:s Fair Information Practices samt Cavoukians egna åsikter om hur integritet bör säkras. Nedan följer de principer som PbD innehåller:

2.4.1 De sju fundamentala principerna

Proactive not Reactive; Preventive not Remedial
Den första principen för Privacy by Design handlar om att agera proaktivt och förebygga personuppgiftsincidenter innan de uppkommer. PbD väntar inte på att personuppgiftsincidenter ska inträffa och erbjuder inte heller lösningar när de inträffat. Istället

ämnar det att förebygga att det händer från första början (Cavoukian, 2009). För att agera proaktivt säger Cavoukian (2009) att det krävs ett tydligt engagemang från högsta ledning. De bör implementera och påtvinga höga standarder för integritet, gärna högre än de som redan gäller enligt lag. Ledningen bör också främja detta engagemang och andra integritetsåtaganden till övriga delar av organisationen för att skapa en företagskultur som reflekterar detta synsätt. Slutligen bör organisationen anamma metoder för att identifiera dåliga integritetsåtaganden för att kunna korrigera eventuella negativa effekter innan de inträffar. Detta bör göras på ett proaktivt, systematiskt och innovativt sätt (Cavoukian, 2009).

Privacy as the Default
Den andra principen för PbD ämnar säkerställa att integritetsskydd finns och används som standard i IT-system eller företagsprocesser. Användaren ska inte behöva agera för att skydda sina personuppgifter (Cavoukian, 2009). Till denna princip har Cavoukian (2009) valt att applicera följande FIP:s (”Fair Information Practices”) för att beskriva vad den innehåller.

- **Purpose Specification –** Anledningen till behandlingen av personuppgifter ska kommuniceras till individen i fråga innan eller i samband med insamlingen. Syftet ska också vara tydligt, begränsat och relevant för den aktuella behandlingen (Cavoukian, 2009).

- **Collection Limitation –** Insamlingen av personuppgifter ska vara begränsad till syftet för insamlingen och måste genomföras rättvist och lagligt (Cavoukian, 2009).

- **Data Minimization –** Insamling av uppgifter som kan identifiera en person ska hållas till ett minimum. När mjukvara designas bör man använda interaktioner och transaktioner som inte kräver uppgifter som kan identifiera en individ. Identifiering, observation och möjligheten att sammanlänka personuppgifter bör minimeras där det är möjligt.

- **Use, Retention and Disclosure Limitation –** Personuppgiftsbehandling som individen samtyckt till ska begränsas till det syfte som kommunicerats till denne förutom där det annars kan krävas av lag. Personuppgifter ska bara behandlas så länge de uppfyller syftet för behandlingen och ska därefter förstöras på ett säkert sätt.

Privacy Embedded into Design
Den tredje principen handlar om att PbD ska integreras redan i designen av IT-system eller företagsprocesser. PbD bör inte implementeras som ett tillägg till en redan framtagen produkt eller tjänst eftersom den då inte är en del av huvudfunktionaliteten. För att åstadkomma detta förespråkar Cavoukian (2009) att man bör använda ett holistiskt, integrerat och kreativt synsätt. Detta eftersom man då tar hänsyn till en bredare kontext och alla stakeholders intressen. Som tillvägagångssätt bör accepterade standarder och ramverk från kända institut användas i implementeringen av integritet. Man bör också utföra PIA:s eller ”Privacy Impact Assesments” och publicera dess resultat (Cavoukian, 2009). Slutligen säger Cavoukian (2009) att en organisation bör säkerställa att de negativa effekterna av en teknologi eller process relaterat till integritet, minskas så mycket det bara går och att effekterna inte kan påverkas genom användarfel.

Full Functionality – Positive-Sum, not Zero-Sum
PbD direkt motsätter sig en syn där den påverkar andra intressen såsom design eller tekniska möjligheter. Målet är istället att skapa en ”win-win” situation där alla intressen tillgodoses

(Cavoukian, 2009). PbD förespråkar därför hög kreativitet och god innovation för att uppnå full funktionalitet samtidigt som vikten av tydlig dokumentation, bra mätstockar och väl definierade funktioner understryks (Cavoukian, 2009).

End-to-End Security – Lifecycle Protection
Pbd förespråkar att integritet kontinuerligt skyddas under hela livscykeln för alla insamlade personuppgifter. Cavoukian (2009) lägger extra vikt vid datasäkerhet och poängterar att det inte bör finnas några luckor i vare sig skydd eller ansvar. Alla entiteter som behandlar personuppgifter måste ta ansvar för dem genom hela livscykeln. Från att de samlas in tills de uppfyllt sitt syfte och förstörs på ett säkert sätt. För att skydda personuppgifterna bör entiteterna använda sig av erkända standarder och tillämpa metoder såsom kryptering, stark åtkomstkontroll och loggning (Cavoukian, 2009).

Visibility and Transparency
För att få eller bibehålla intressenters förtroende, för att en teknologi eller företagsprocess fungerar som tidigare påstått, är det viktigt att ge dem insyn och tillhandahålla en oberoende verifikationsprocess (Cavoukian, 2009). För att uppnå en hög grad av transparens bör specifika individer tilldelas ansvar för integritets relaterade produkter samt att information om dessa produkter bör göras tillgängliga för allmänheten (Cavoukian, 2009). En organisation bör också enligt Cavoukian (2009) implementera mekanismer för att hantera klagomål och för att få upprättelse. Information om dessa ska kommuniceras till individen (Cavoukian, 2009).

Respect for User Privacy
Den sjunde och sista principen för PbD sätter användaren rakt i fokus och stryker under att respekt för användares integritet är bland det viktigaste. Cavoukian (2009) säger att ett av de mest effektiva sätten att förhindra missbruk av personuppgifter är att låta användaren få en aktiv roll i hanteringen av sin egen information. För kunna respektera användares integritet är det viktigt att införskaffa deras samtycke till behandling. Samtycket ska vara tydligare och mer specifikt i takt med att de insamlade uppgifterna blir mer känsliga (Cavoukian, 2009). Uppgifternas korrekthet, individens tillgång till dem och mekanismer för prövning och klagomål omnämnas också av Cavoukian (2009) som viktiga FIP:s att förhålla sig till om man vill respektera användaren enligt PbD. Slutligen poängterar Cavoukian (2009) att oavsett om det gäller en teknisk produkt eller en företagsprocess så ska användaren alltid kunna ta ett informerat beslut om sin integritet och därför bör individens intressen alltid stå i fokus.

2.4.2 Utmaningar med Privacy by Design

Alshammari och Simpson (2017) skriver att Privacy by Design saknar holistiska och systematiska metoder för att hantera komplexiteten och variationen av integritetsproblem. Författarna säger också att det saknas stöd för att transformera PbDs principer till krav och aktiviteter för systemutvecklare. De skriver dock att detta kan beror på PbDs omfattande natur och att det på så vis är förståbart men en konsekvens är då att principerna blir väldigt abstrakta. Gürses, Troncoso och Diaz (2011) beskriver samma fenomen genom att säga att principerna är vaga och att de är svåra att applicera på utvecklingen av system. Principerna är också rekursiva i sin utformning eftersom de innehåller termen ”Privacy by Design”, vilket i förlängningen innebär att ”privacy by design means applying privacy by design” (Gürses, Troncoso & Diaz, 2011). Detta skapar en otydlighet, enligt författarna, eftersom det är svårt för läsaren att förstå vad integritetsproblemet är och hur det ska översättas till utvecklingskrav (Gürses, Troncoso & Diaz, 2011).

Många av utmaningarna med PbD ligger främst kring transformeringen av PbD:s principer till faktiska implementerbara krav eller aktiviteter (Alshammari & Simpson, 2017; Bu et al., 2020; Chen & Williams, 2013; Gürses, Troncoso & Diaz, 2011; Spiekermann, 2012). Bednar, Spiekermann och Langheinrich (2019) beskriver också svårigheterna med att få jurister och systemutvecklare att samarbeta i relation till de legala krav som finns för integritet. I deras studie visade det sig att systemutvecklarna kände att de legala kraven inte var tydligt definierade ännu och inte förens ett etablerat legalt ramverk var på plats kunde individer få sin integritet (Bednar, Spiekermann & Langheinrich, 2019). Spiekermann (2012) poängterar att en stor tillgång i många företags affärsmodeller idag är personuppgifter. Ledningens aktiva engagemang i företagens integritetsstrategi blir således en nyckelfaktor, vilket författaren uttrycker som en av utmaningarna för verksamheter (Spiekermann, 2012).

Van Rest et al. (2014) har dock ytterligare en infallsvinkel och säger att Cavoukians angreppssätt kan bli problematisk för individen och samhället i stort. Författarna skriver att Cavoukian antar en evolutionär ansats där näringsliv och privata konsumenter tillsammans listar ut vad som fungerar och inte. Enligt författarna leder detta till att innovation främjas men att det kan komma till bekostnad av transparens. Om varje kommersiell entitet själva får tolka och välja hur de ska implementera PbD måste också privata konsumenter, lokala myndigheter och beslutsfattare förstå skillnaden mellan olika entiteters tillvägagångssätt (van Rest et al., 2014).

2.4.3 Möjligheter med Privacy by Design

Privacy by Design har också incitament för att företag ska bruka det. Som Cavoukian och Chibba (2018) skriver handlar det till stor del om att införskaffa och behålla konsumenters förtroende. Deras argument bygger på att tillit leder till lojalitet och lojalitet leder till upprepade affärer och högre omsättning. Författarna understryker också de negativa konsekvenserna av bruten tillit, vilket kan leda till förlorade marknadsandelar och lägre omsättning.

Cavoukian (2010) beskriver hur företag kan uppnå en intern kultur med integritet i fokus genom att se integritetsproblem som ett verksamhetsproblem och inte bara som ett problem i fråga om att efterleva lagar och regler. Cavoukian (2010) menar att detta synsätt leder till ett ”win-win” scenario.

> The ultimate results—which are highly desirable—include enhanced trust, improved efficiencies, greater innovation, and a heightened competitive advantage. Privacy is good for business (Cavoukian, Taylor & Abrams, 2010).

Bu et al. (2020) motiverar integritetsinitiativ genom att påpeka de negativa konsekvenserna som kan följa av ett dåligt integritetsarbete. Författarna skriver att konsekvenser från dataläckor ökar i allvarlighet om företag är för beroende av persondata. Bednar, Spiekermann och Langheinrich (2019) säger också att rapporter från 2016–2017 avslöjat att det skett hundratals dataläckor som har inneburit att miljontals personuppgifter har avslöjats. Tidigare läckor har också haft stor negativ ekonomisk påverkan på företag och kunder samt att det försämrar hela industrins rykte (Bu et al., 2020).

2.4.4 Lösningar och andra tillvägagångssätt

Många av de författare som kritiserat PbD på olika sätt har själva lämnat förslag på lösningar eller andra tillvägagångssätt för hantering av integritetsfrågor. Kroener och Wright (2014) redogör för en mer organisationsomspännande lösning. Författarna föreslår att organisationer ska följa en uppsättning principer. Det kan då röra sig om till exempel de principer som Cavoukian (2012) presenterat eller de sex principer Schaar (2010) tar upp i sin artikel som även den går under namnet ”Privacy by Design”. Organisationer bör också enligt Kroener och Wright (2014) implementera processriktlinjer. Här föreslår författarna att Privacy impact assessments används (PIA:s), vilket går hand i hand med vad Van Lieshout et al. (2011) skriver. Van Lieshout et al. (2011) säger att PIA:s bidrar med ett strukturerat och systematiskt arbetssätt för att hantera organiseringen av ansvar i en organisation. Det tänkta syftet med PIA:s är dock lite annorlunda enligt Kroener och Wright (2014) när de säger att PIA:s kan användas för att identifiera integritetsrisker och på så sätt veta vart integritetsprinciper som PbD kan appliceras. När Kroener och Wright (2014) publicerade ”A Strategy for Operationalizing Privacy by Design” rekommenderade de en kommande ISO standard för hantering av PIA:s. Idag är denna standard publicerad under ISO/IEC 29134:2017. Avslutningsvis föreslår författarna att organisationer bör använda en rad tekniska hjälpmedel vid integreringen av integritet i nya teknologier, system eller tjänster (Kroener & Wright, 2014).

Senarath och Arachchilage (2018) tar ett annat perspektiv och fokuserar enbart på lösningar som underlättar för utvecklare. Författarna föreslår förenklade och tydliga integritetsriktlinjer som också ska vara mätbara och på så sätt gå att utvärdera. Författarna föreslår också att utvecklare bör genomgå utbildning relaterad till integritet, eftersom de funnit att utvecklares brist på integritetskunskap hindrar dem ifrån att effektivt implementera integritet i utvecklingen av mjukvara. Slutligen föreslår Senarath och Arachchilage (2018) att integritetskrav ska vara specificerade med mjukvarutekniker så att utvecklare enklare kan hitta en passande teknik, t.ex. anonymisering, för ett integritetskrav.

Alshammari och Simpson (2017) nöjer sig inte med enbart ett organisationstäckande perspektiv utan en av de fyra principerna de presenterar är på makronivå. Den första principen innebär att applicera ett set av universellt överenskomna integritetsprinciper. Författarna föreslår användningen av GPS, eller Global Privacy Standards som Cavoukian (2006) presenterade, i kombination med principerna Hansen, Jensen och Rost (2015) presenterade under ”IEEE Security and Privacy Workshops” 2015. Nästa princip Alshammari och Simpson (2017) introducerar är en livscykelmodell för personuppgifter som ska inkludera personuppgifter, associerad metadata, relaterade aktörer och stödjande mjukvarusystem. Syftet med modellen är enligt författarna att kunna säkerställa integritet och för att kunna uppvisa efterlevnad av de legala krav som är applicerbara. Modellen är till för att organisationer enklare ska kunna identifiera risker i de olika stegen personuppgifter generellt kan befinna sig i; insamling, lagring, användning, avslöjande och förstörelse. Den tredje principen syftar till att se integritetsrisker i sin helhet. Principen går ut på att applicera en sammanslagning av två existerande ramverk; ”the taxonomy of privacy” och ”the contextual integrity framework”. Genom att slå samman dessa ramverk säger Alshammari och Simpson (2017) att organisationer enklare kan transformera legala, sociala och politiska perspektiv till operativa krav som kan implementeras i system. Tanken är också enligt författarna att detta ska hjälpa organisationer att identifiera, analysera och utvärdera integritetsrisker under de steg som inkluderas i livscykeln för personuppgifter. Alshammari och Simpson (2017) presenterar slutligen den sista principen som är mer i linje med vad Senarath och Arachchilage (2018)

presenterade. Principens huvudsakliga syfte är att tydligare illustrera vilka integritetskrav som passar en specifik mjukvaruarkitektur (Alshammari & Simpson, 2017). Principen ska framför allt visa när det passar att använda sig av specifika arkitekturmönster, designmönster och andra tekniska hjälpmedel såsom PET:s (Privacy Enhancing Technologies). Detta ska åstadkommas genom att implementera design strategier som tar hänsyn till principerna i PbD (Alshammari & Simpson, 2017).

2.5 General Data Protection Regulation

Dataskyddsförordningen, på engelska General Data Protection Regulation eller förkortat GDPR, trädde i kraft den 25 maj 2018. GDPR ämnar att fastställa bestämmelser som avser behandling av personuppgifter för fysiska personer och på så sätt skydda fysiska personers fri- och rättigheter (EU, 2016, artikel 1). I samband med införlivandet av GDPR upphävdes också direktiv 95/46/EG, tidigare känt som Dataskyddsdirektivet (EU, 2016, artikel 94). Förarbeten och tidigare utkast till dataskyddsförordningen omnämner också Privacy by Design (EU, 2012).

2.5.1 Skäl 78 & Artikel 25

Skäl 78 i GDPR uppmanar organisationer att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda fysiska personers fri- och rättigheter samt för att möta kraven i GDPR. För att visa att GDPR efterlevs bör organisationer anta interna strategier och vidta nödvändiga åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard (EU, 2016). Skäl 78 listar även åtgärder i en icke uttömmande lista, som organisationer kan anta för att uppfylla principerna (EU, 2016).

Artikel 25 om principerna för inbyggt dataskydd och dataskydd som standard förbinder organisationer att vidta lämpliga tekniska och organisatoriska åtgärder för genomförandet av dataskyddsprinciperna (mer om dessa i punkt 2.4.2) (EU, 2016). I Artikel 25 finns också ett fokus på principen om uppgiftsminimering, vilket innebär att endast personuppgifter som är nödvändiga för ändamålen med behandlingen, ska behandlas. Artikel 25 klargör att uppgiftsminimering även ska gälla mängden insamlade personuppgifter, behandlingens omfattning, tiden uppgifterna lagras och att de inte görs tillgängliga för ett obegränsat antal personer (EU, 2016).

Viktigt att tillägga är att punkt 3 i artikel 25 säger att godkända certifieringsmekanismer som beskrivs i artikel 42 får användas för att visa att kraven i övriga delar av artikel 25 uppfylls.

2.5.2 Artikel 5 & 6

Artikel 5 i dataskyddsförordningen handlar om de principer den personuppgiftsansvarige är skyldig att följa vid behandling av personuppgifter (EU, 2016). Nedan följer en kort beskrivning av dessa principer:

Laglighet, korrekthet & öppenhet

Ändamålsbegränsning

Uppgifter får endast samlas in för uttryckligen angivna och berättigade ändamål och inte senare behandlas för andra ändamål som är oförenliga med ursprungs ändamålen (EU, 2016).

Uppgiftsminimering
Uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen för insamlingen (EU, 2016).

Korrekthet
Uppgifter ska vara korrekta och uppdateras om det behövs. Uppgifter som inte överensstämmer med ändamålen för insamlingen ska raderas eller rättas utan dröjsmål (EU, 2016).

Lagringsminimering
Uppgifter för inte lagras så de kan identifiera en registrerad under en längre tid än det som är nödvändigt för ändamålen med behandlingen (EU, 2016).

Integritet och konfidentialitet
Uppgifter som ska behandlas måste ha lämpliga skyddsåtgärder mot till exempel obehörig – och otillåten behandling, mot förlust, förstöring eller skada genom olyckshändelse (EU, 2016).

Ansvarsskyldighet
Personuppgiftsansvarige ska ansvara för efterlevnaden av samtliga principer och måste kunna visa att de efterlevs (EU, 2016).

Artikel 6 i dataskyddsförordningen redogör för de grunder, även kallade rättsliga grunder, som måste vara uppfyllda för att behandlingen ska anses vara laglig (EU, 2016). Endast en av dessa grunder måste dock uppfyllas för att en personuppgiftsansvarig ska kunna behandla uppgifter lagligt. Grunderna innehåller samtycke, avtals fullgörande, rättslig förpliktelse, människors vitala intressen, allmänt intresse eller led i myndighetsutövning, och intresseavvägning (EU, 2016).

2.5.3 Avsnitt 2 & 3

Avsnitt 2 och 3 i dataskyddsförordningen redogör för de olika rättigheter som den registrerade har i förhållande till behandlingen av deras personuppgifter (EU, 2016). Avsnitt 2 inleds med artikel 13 och 14 som beskriver den skyldighet en personuppgiftsansvarig har att lämnat ut information till den registrerade innan eller i samband med insamlingen av personuppgifterna (EU, 2016). Informationen ska bland annat innehålla den personuppgiftsansvariges identitet och kontaktuppgifter, ändamålen för behandlingen och den rättsliga grund som behandlingen åvilar. Artikel 15 beskriver sedan den rätt en registrerad har att få tillgång till sin information (EU, 2016). Artikel 15 kan upplevas som väldigt lik artikel 13 och 14 men där finns betydande skillnader. I artikel 15 ska information om vilka kategorier av personuppgifter som behandlas lämnas ut, oavsett om uppgifterna samlats in direkt från den registrerade. De undantag som gäller för artikel 13 och 14 är inte heller tillämpliga på artikel 15 (EU, 2016). Avsnitt 3 redogör för ytterligare rättigheter den registrerade har. Rättigheterna inkluderar: rätten till rättelse, rätten till radering, rätten till begränsning och rätten till dataportabilitet (EU, 2016).

2.6 Litteratursammanfattning

Tabell 1: **Karaktären hos PbDs principer**, visar vad Privacy by Designs olika principer kan karaktäriseras av för aktiviteter, metoder och andra åtaganden. Karaktärsdragen är översatta och tolkade från Cavoukians egna beskrivning av principerna samt de FIP:s som principerna är associerade med.

Tabell 1: Karaktären hos PbDs principer

Principer	**Karaktäriseras av**
Proactive not Reactive; Preventative not Remedial	• Engagemang från ledning • Högre nivå av integritet än lagar och andra juridiska krav • Etablerade metoder för att känna igen dålig integritetsdesign och dålig integritetspraxis • Ett integritetsåtagande som delas av användargrupper och intressenter
Privacy Embedded into Design	• Ett systemiskt, principfast sätt att integrera integritet bör antas • När det är möjligt bör en detaljerad PIA och riskbedömning genomföras och publiceras • Integritetseffekterna av den resulterande tekniken, driften eller informationsarkitekturen och deras användning, bör bevisligen minimeras och inte lätt försämras genom användning, felkonfiguration eller fel.
Full Functionality – Positive-Sum, not Zero-Sum	• När integritet integreras i en teknik, process eller ett system ska det göras på ett sådant sätt att full funktionalitet behålls, och i största möjliga utsträckning, att alla krav är optimerade. • Integritet positioneras ofta som att behöva konkurrera med andra legitima intressen, designmål och tekniska möjligheter inom en viss domän. Privacy by Design avvisar ett sådant tillvägagångssätt - det omfattar legitima mål och tillgodoser dem i en innovativ positiv helhet. • För att hitta en lösning som möjliggör multifunktionalitet ska alla intressen och mål vara tydligt dokumenterade, önskade funktioner artikulerade, mått överenskomna och avvägningar avvisade eftersom de ofta är onödiga.

End-to-End Security – Lifecycle Protection	• Säkerhet
	  ○ Ansvar genom hela livscykeln och stämma överens med erkända standarder på området
	• Applicerad säkerhet
	  ○ Konfidentialitet, integritet och tillgänglighet genom hela livscykeln.
	• Metoder för säker förstöring, lämplig kryptering, och starka åtkomstkontroll- och loggnings metoder.

Privacy as the Default	• Syftes specifikation

	• Insamlingsbegränsning • Dataminimering • Begränsning av användning, lagring och avslöjande
Visibility and Transparency	• Ansvarighet • Öppenhet • Efterlevnad
Respect for User Privacy	• Samtycke • Exakthet • Tillgång • Efterlevnad

Tabell 2: **Utmaningar & möjligheter** visar en sammanställning av de utmaning och möjligheter som vi identifierat i den tidigare forskning som vi har gått igenom. För att öka tydligheten har vi färgkodat cellerna. Den röda färgen representerar *Utmaningar* och den gröna färgen representerar *Möjligheter*.

Tabell 2: Utmaningar & möjligheter

Utmaningar	**Relaterad litteratur**
Relation och kommunikation mellan olika parter inom organisationen.	Bednar, Spiekermann och Langheinrich (2019)
Privacy by Design saknar holistiska och systematiska metoder för att hantera komplexiteten och variationen av integritetsproblem.	Alshammari och Simpson (2017)
PbDs abstrakta/vaga/otydliga principer leder till att transformeringen av PbDs principer till faktiska implementerbara krav eller aktiviteter blir komplicerad.	Alshammari och Simpson (2017), Gürses, Troncoso och Diaz (2011), Bu et al., (2020), Chen & Williams (2013), Spiekermann (2012)
Ledningens aktiva engagemang i företagens integritetsstrategi.	Spiekermann (2012)
Evolutionär ansats kan leda till att innovation främjas men till bekostnad av transparens	van Rest et al., (2014)
Möjligheter	**Relaterad litteratur**
Ökat förtroende	Cavoukian och Chibba (2018)
Lägre risk för känsliga dataläckor	Bu et al. (2020), Bednar, Spiekermann & Langheinrich (2019)

3 Tillvägagångssätt

3.1 Litteraturgenomgång

När vi beslutat oss för att studera Privacy by Design inledde vi arbetet med att undersöka tidigare litteratur på områdena Privacy by Design, integritet och dataskyddsjuridik. Med detta inledande arbete identifierade vi bland annat nyckelförfattare, artiklar, ramverk och teorier för Privacy by Design. Litteraturen vittnar om att det finns en problematik med PbD till följd av avsaknaden av en tydlig metodologi både för att implementera (Chen & Williams, 2013; Spiekermann, 2012) men även för att mäta PbD i organisationer (Kroener & Wright, 2014). Tidigare studier har gjorts i syfte att identifiera ett tillvägagångssätt eller guide för implementationen av PbD (Alshammari & Simpson, 2017; Spiekermann & Cranor, 2009). Stort fokus har däremot legat på utvecklarna (Bednar, Spiekermann & Langheinrich, 2019; Hadar et al., 2018; Senarath & Arachchilage, 2018). Detta fokus på utvecklarna skulle kunna bero på att det är de som anses vara de direkta implementerarna av PbD (Bu et al., 2020).

PbD förespråkar en organisationsomspännande omfattning och en av de huvudsakliga utmaningarna med Privacy by Design är att involvera organisationens ledning i integritetsstrategin (Spiekermann, 2012). Av denna anledning började vi fundera på hur personer i en ledande roll och deras organisation arbetar med PbD för att exempelvis främja och skapa förståelse för ansatsen ut i organisationens operativa delar.

För att hitta relevant litteratur för studien har vi främst använt oss av Google Scholar och Lunds universitets sökmotor LUBsearch. Referensförteckningen i artiklarna användes för att hitta bakomliggande studier som i flera fall även kom att bli relevant för oss. För att säkerställa ett pålitligt material har vi tittat på bland annat antal citationer, återkommande författare samt källor i redan etablerat material.

Nedan är en lista på några av de nyckelord som vi har använt oss av i sökandet, vilka har använts för sig men även i kombination med varandra. Till höger om nyckelordet är antalet träffar i de olika sökmotorerna.

- PbD – 205,000 (Google Scholar), 7589 (LUBsearch)
- Privacy vs Security- 3,520,000 (Google Scholar), 757 (LUBsearch)
- Privacy by design – 4,930,000 (Google Scholar), 43,921 (LUBsearch)
- "privacy by design" empirical – 3900 (Google Scholar), 22 (LUBsearch)
- Privacy managers – 2,310,000 (Google Scholar), 6181 (LUBsearch)
- FIP – 278,000 (Google Scholar), 7131 (LUBsearch)

3.2 Metodval

Vi har studerat hur arbetet med integritet ser ut för personer i en ledande roll och deras organisation samt hur detta arbete förhåller sig till ansatsen Privacy by Design.

Studiens forskningsfråga är: *Hur förhåller sig integritetsarbetet hos personer i en ledande roll och deras organisationer till ansatsen Privacy by Design?*

För att besvara forskningsfrågan behöver vi således en forskningsmetod som ger oss möjlighet att förstå vad arbetet med integritet i förhållande till PbD innebär för en person i en ledande roll och dennes organisation.

Termen PbD har utmålats för att vara för vag för att förstås av utvecklare (Bu et al., 2020). Begreppet har däremot blivit allmänt känt inom sfären för integritetsarbete, inte minst efter att det införlivats av regelverk såsom GDPR. Detta betyder däremot inte att PbD är någonting som en person i en ledande roll nödvändigtvis måste ha en stor förståelse för. Det är därför viktigt att poängtera att våra intervjupersoner inte är titulerade som experter på området Privacy by Design. Förståelsen för och arbetet med Privacy by Design kan således variera mellan respondenterna och detta ansåg vi vara viktigt att beakta vid val av metod.

Privacy by Design som ansats är komplex och abstraktionsnivån på begreppet är hög. För att besvara forskningsfrågan har vi valt att hålla intervjuer. Intervjuer ger oss möjlighet att generera detaljerad information om respondenternas erfarenheter samt även möjlighet att ställa komplexa och öppna frågor (Oates, 2006). Frågorna kan komma att behöva anpassas dels efter respondenternas roller inom den organisation som de företräder. Och dels efter intervjupersonernas förståelse för Privacy by Design som ansats.

För att besvara forskningsfrågan krävs att vi sätter oss in i intervjupersonernas erfarenheter och upplevelser, en lämplig ansats är då enligt Schultze & Avital (2011) en kvalitativ intervjubaserad studie då syftet med en sådan är att beskriva och förtydliga människors tidigare erfarenheter. För att generera så detaljerade empiriska data som möjligt har intervjuerna genomförts semi-strukturerat. Detta ger oss utrymme att ställa följdfrågor på intressanta aspekter som vi kanske inte har förberett frågor för, men ger även intervjupersonerna möjlighet att prata mer detaljerat och ta upp egna åsikter eller erfarenheter som de tycker kan vara relevant för studien, vilket är i linje med Oates (2006) rekommendationer.

3.3 Urval

3.3.1 Val av organisation

Vi ansåg det vara lämpligt att leta efter organisationer som omfattas av GDPR. Detta ger organisationen ett regelverk att följa och vi kunde därför ha som utgångspunkt att det sker någon form av integritetsarbete hos organisationen. Med detta sagt letade vi alltså efter organisationer som arbetar med att utveckla någon form av it-artefakt eller tjänst som i någon mån är riktad mot privatpersoner alternativt samlar in data om privatpersoner.

Titlar såsom SCRUM-master, avdelningschef, landschef, CDO, CIO, CTO och produktägare har legat till grund för vårt urval då vi anser att dessa roller passar in på personer som blivit tilldelade ett formellt ledarskap. Vi strävade efter att hitta intervjupersoner med olika roller för att få en bredare uppfattning om hur integritetsarbete kan se ut hos olika organisationer. Vi ansåg också att intervjupersonerna behövde vara kunniga inom integritetsfrågor. De behövde

besitta en relativt hög hierarkisk position i sin verksamhet samt att de själva varit delaktiga i integritetsrelaterade arbeten.

Vi hörde av oss till totalt 35 personer. 12 personer kontaktades via LinkedIn och 23 personer kontaktades via mejl. Av de 35 personer som vi kontaktade var det 12 personer som återkopplade till oss. 4 av personerna hade inte tid eller möjlighet att delta i en intervju och 4 av personerna kom vi fram till inte uppfyllde de kriterier vi hade på dem som intervjupersoner. En av personerna som kontaktades via LinkedIn kände själv att hen inte hade tillräckligt med konkreta arbetsuppgifter för att kunna applicera på vårt forskningsområde men personen tipsade i stället om en person i hens kontaktnät som senare kom att ställa upp på en intervju.

Totalt hade vi då fyra personer som passade väl in på våra kriterier samt hade möjlighet att ställa upp på en intervju. Kort därpå fick vi ett oväntat och mycket tråkigt besked om att en av personerna som vi skulle intervjuat plötsligt gått bort under oklara omständigheter. Därmed hade vi totalt 3 personer kvar som passade in och kunde ställa upp på en intervju.

3.3.2 Val av intervjuperson

Tabell 3: **Intervjusubjekt & Organisationer** nedan, ger en översikt över våra respondenter.

Tabell 3: Intervjusubjekt & Organisationer

Intervjusubjekt	Organisation/Bransch	Yrkesroll / Titel	Längd på intervju	Datum och tid	Appendix
IS1	Bank	Principal Architect Software IT l IT Strategy & Architecture	Ca 50 minuter	22-april-2021, 13:00-14:00	A
IS2	Ad-Tech	Produktchef	Ca 45 minuter	23-april-2021, 13:00-14:00	B
IS3		Frilansande IT-Konsult	Ca 38 minuter	27-april-2021, 13:00-14:00	C

Banken arbetar med finansiella tjänster till privat och företagsmarknaden. Banken arbetar med exempelvis olika betallösningar (retail finance), factoring, utlåning och inlåning, kreditkort och privatlån. På banken arbetar IS1 som Principal Architect på avdelningen IT-strategi och arkitektur. IS1 är med och sätter de ramar som banken har när de utvecklar sina tjänster. Detta kan vara att sätta policys, guidelines och vilka regler som banken måste följa.

Ad-Tech är en förkortning av advertising technology. Begreppet hänvisar till olika typer av analyser eller digitala verktyg som hjälper företag att annonsera smartare på nätet. På Ad-

tech-bolaget arbetar IS2 som produktchef och sitter med i management teamet tillsammans med VD, finanschef, säljchef, marketingchef osv. Enligt IS2 så är ad-tech-industrin en industri som samlar in extremt mycket data om konsumenter (Appendix C, #10). Ad-tech-bolaget finns med deras annonsering på stora publicisters sajter såsom nyhetssajter.

Frilansande IT-Konsult: IS3 arbetar primärt med utveckling av olika system för kunders räkning. Hen ansvarar bland annat för att sätta ihop och rekrytera utvecklingsteam och besitter det övergripande produktansvaret.

3.4 Intervju

När vi skulle välja om intervjun skulle ske på distans eller om vi skulle möta alla deltagarna fysiskt, insåg vi snabbt att vi inte hade mycket val. Eftersom studien genomfördes under april och maj 2021 under en pandemi (Covid-19), har vi inte haft möjlighet att besöka våra intervjupersoner fysiskt och har därför varit tvungna att utföra intervjuerna på distans. Jacobsen (2002) skriver att intervjuer som utförs ansikte mot ansikte är att föredra, speciellt vid öppna frågor eftersom intervjupersonerna då tycks ha lättare att prata om känsliga ämnen. Jacobsen (2002) tillägger också att vid intervjuer per telefon är det lättare för intervjupersonerna att ljuga. Dessutom förlorar intervjuaren möjligheten att observera intervjupersonens kroppsspråk (Jacobsen, 2002).

Med ovanstående som bakgrund valde vi att utföra intervjuerna över kommunikationsverktyg som tillät videosamtal. På så sätt kommer vi så nära den fysiska intervjun vi kan komma under rådande omständigheter och bibehåller förhoppningsvis de fördelar som finns med det tillvägagångssättet.

3.4.1 Pilotintervju

För att förbereda oss för de kommande intervjuerna utförde vi ett flertal pilotintervjuer. Syftet med pilotintervjuerna var att känna in oss i rollen som intervjuledare och att säkerställa att vi följer de punkter Oates (2006) tar upp i samband med intervjuer. Eftersom intervjuerna skulle utföras på distans med tekniska hjälpmedel var vi också tvungna att kontrollera att de fungerade som tänkt. De krav vi hade på de tekniska hjälpmedlen var att vi skulle kunna spela in intervjun. Framför allt ljudet var av intresse men gärna video också, samt att vi skulle kunna schemalägga intervjuerna och skicka en inbjudan till intervjupersonerna.

För den första pilotintervjun (P1) använde vi Microsoft Teams. MS Teams fungerade väl att spela in i så vi fortsatte P1 genom att en av författarna agerade intervjusubjekt och den andra intervjuledare. När vi var nöjda med P1s innehåll avbröt vi intervjun för att kontrollera de andra kraven vi hade på MS Teams. Det visade sig att MS Teams lagrade inspelningen av intervjun online i molnet, vilket var problematiskt av två skäl. Först innebar det att vi var tvungna att kontroller att det var godkänt av intervjupersonerna att lagra intervjun i molnet och sedan att det fanns en begränsning på hur mycket data vi kunde lagra. Vi lyckades inte heller schemalägga intervjuerna och bjuda in våra intervjusubjekt i MS Teams även om programvaran ska stödja de funktionerna.

Den andra pilotintervjun (P2) fokuserade mer på att lösa de tekniska problemen vi upplevt med P1. Vi valde därför att undersöka Google Meet. Med Google Meet lyckades vi snabbt

schemalägga intervjuerna och skicka inbjudningar som vi inte kunde i P1. Tyvärr krävdes en annan licens för att spela in intervjuerna.

Slutligen utförde vi pilotintervju tre (P3), där vi utforskade de tekniska funktionerna i Zoom. Vi var initialt skeptiska till att använda Zoom eftersom det tidigare rapporterats om olika säkerhetsbrister. Av den anledningen kontrollerade vi alltid med intervjusubjektet att de accepterade användningen av Zoom samt att vi vidtog olika säkerhetsåtgärder som lösenordsskydd och låsta möten, för att minska risken för intrång. Zoom uppfyllde dock alla andra krav vi ställt. Vi kunde enkelt schemalägga möten och bjuda in intervjusubjekten med en URL. Vi kunde också spela in mötena och spara de lokalt på våra datorer. En adderad bonus var att båda intervjuledarena kunde spela in intervjun individuellt. Vilket minskade risken för dataförlust- eller korruption.

3.4.2 Intervjuguide

Den övergripande intervjuguiden har utformats i enlighet med de riktlinjer Oates (2006) framför. Den består av 8 segment där vi i det inledande segmentet introducerar oss själva och vår uppsats. I det andra segmentet fokuserar vi på att informera intervjupersonen om de etiska förpliktelserna som föreligger. Det tredje segmentet består av inledande och enkla frågor, vars syfte är att samla in grundläggande information och hjälpa oss att värma upp intervjupersonen. Det fjärde, femte och sjätte segmentet är våra huvudområden. Huvudområdena inleds med övergripande frågor om integritet för att sedan dyka djupare in på intervjupersonens åsikter och arbete. Frågor om ”Utmaningar och möjligheter” ställs även löpande under ”PbD:s principer” för att enklare relatera exempelvis en utmaning med en specifik princip, men också för att intervjupersonen inte ska ha glömt bort det till nästa segment. Det sjunde segmentet består av övriga frågor där intervjupersonen för chansen att lägga till andra insikter som inte tidigare nämnts och det åttonde och sista segmentet avslutar intervjun.

Intervjuguiden har utvärderats och förbättrats lite efter varje intervju för att på ett bättre sätt få fram den informationen vi ansåg var relevant. Det har främst rört sig om ordningen på frågorna samt nya följdfrågor för att få ut mer av vissa svar.

Tabell 4: Övergripande intervjuguide

Område	Exempelfrågor & Viktiga punkter

Välkommen, forskningsfråga och syfte	• Presentation
	  ○ av oss
	  ○ forskningsfråga
	  ○ syfte

Etiska aspekter av intervjun	• Samtycke till inspelning • Anonymitet (individ och/eller organisation) • Försäkran om insamlat material ○ Används endast för studien • Rätt att avbryta intervjun • Tillgång till transkribering och färdig uppsats

Bakgrund	• Ålder, utbildning
	• Vad är din nuvarande roll på (Företag X)?
	  ○ Har du haft andra roller på (Företag X)?
	  ○ Tidigare roller i din karriär?
	• Hur länge har du jobbat för (Företag X)?
	• Berätta lite om (Företag X).

Inledande frågor	• Hur ser du på begreppet privacy? • Anser du att ni arbetar med privacy by design som ansats? • Varför arbetar ni med integritetsfrågor?
PbD:s principer	• Se Tabell 5: **Intervjuguide**
Utmaningar & möjligheter	• Ytterligare utmaningar eller möjligheter som inte tagits upp tidigare?
Övrigt	• För studien relevanta tillägg som inte berörts tidigare under intervjun? • Andra frågor eller funderingar?
Avslut	• Får vi återkomma med frågor? • Tackar för medverkan, och för den kunskap de delat med sig av.

Tabell 5: Intervjuguide

Princip	Karaktäriseras av FIPs	Exempelfrågor
Proactive not Reactive; Preventative not Remedial	• Engagemang från ledning • Högre nivå av integritet än lagar och andra juridiska krav • Etablerade metoder för att känna igen dålig integritetsdesign, dålig integritetspraxis • Ett integritetsåtagande som delas av användargrupper och intressenter	• Kan du beskriva hur företagskulturen ser ut i relation till integritet? • Hur hög nivå av integritet upplever du att ni uppfyller? • Har ni processer/metoder för att hantera dåliga integritets beslut?
Privacy Embedded into Design	• Ett systemiskt, principfast sätt att integrera integritet bör antas • När det är möjligt bör en detaljerad PIA och riskbedömning genomföras och publiceras • Integritets effekterna av den resulterande tekniken, driften eller informationsarkitekturen och deras användning, bör minimeras och inte lätt försämras genom användning, felkonfiguration eller fel.	• Följer ni ett standardiserat ramverk för att implementera integritet i era företagsprocesser eller tekniska produkter? • Använder ni er av PIAs? • Hur säkerställer ni att effekterna av en teknik eller process inte påverkar dennes integritet?
Full Functionality – Positive-Sum, not Zero-Sum	• När integritet integreras i en teknik, process eller ett system ska det göras på ett sådant sätt att full funktionalitet behålls och att alla krav är optimerade. • Integritet positioneras ofta som att behöva konkurrera med andra legitima intressen, designmål och tekniska möjligheter inom en viss domän. • Alla intressen och mål måste vara tydligt dokumenterade, önskade funktioner artikulerade, mått överenskomna och tillämpas, och avvägningar avvisade eftersom de ofta var onödiga, för att hitta en lösning som möjliggör multifunktionalitet.	• Upplever du att integritet hindrar eller försvårar framtagningen av teknologier eller processer? • Prioriterar ni integritet på samma sätt som t.ex. designmål eller innovativa tekniska lösningar?

End-to-End Security – Lifecycle Protection	• Säkerhet
	  ○ Ansvar genom hela livscykeln och stämma överens med erkända standarder på området
	• Applicerad säkerhet
	  ○ Konfidentialitet, integritet och tillgänglighet genom hela livscykeln.
	• Metoder för säker förstöring, lämplig kryptering, och starka åtkomstkontroll- och loggnings metoder.
		• Säkerställer ni att integritet inte försämras under senare delar av produkten, tjänsten eller processens livscykel?
		• Kan du ge exempel på tekniska säkerhetsåtgärder ni använder, genom hela livscykeln?

3.5 Bearbetning av empiri

För att lättare kunna dra några slutsatser eller överhuvudtaget arbeta med empirin valde vi att transkribera våra inspelade intervjuer. Jacobsen (2002) redogör för vikten av att reducera den insamlade informationen så den blir enklare att förstå och ger en bättre överblick. Eftersom vår uppsats är ämnescentrerad är det inte samma individfokus i analysen (Jacobsen, 2002), vilket har gjort att vi kunnat reducera empirin från stakningar, upprepningar och material som inte alls är relevant för vår frågeställning.

Samtliga intervjusubjekt har valt att vara anonyma vilket har lett till att vi i vissa stycken av transkriberingarna har fått sänka detaljnivån på deras svar så att de inte kan bli indirekt eller direkt identifierade (Jacobsen, 2002).

3.5.1 Transkribering och kodning

När intervjuerna var transkriberade kunde vi börja koda dem för att hitta de områden som relaterar till uppsatsens undersökningsområde. Vi inledde alltid kodningen genom att analysera transkriberingarna separat för att sedan kunna korskontrollera resultaten tillsammans. Vi har gjort vårt bästa för att tolka intervjusubjektens svar och placera dem i de avsedda områdena.

I Tabell 6: **Kodningsmall** nedan, visas de olika områden som vi identifierat genom vår litteraturgenomgång samt några ytterligare som vi lade till under analysen av intervjuerna. ”Motivering” eller syfte till behandling var ett område som vi tidigare inte tänkt på. Vi upptäckte under intervjuerna att motivering var nära relaterat till ”Möjligheterna” med PbD. Av den anledningen valde vi att slå samman dessa områden. ”Övrigt” användes för att markera information som var relevant för att beskriva vår intervjuperson och dennes organisation.

Kodningen utfördes genom att markera och färglägga meningar i texten som innehöll relevant data för vår studie. På så viss var det väldigt exakt vilket område en specifik mening relaterade till. Det kunde exempelvis se ut så här:

Det är inte så att vi vill vara onda mot kunderna, vi vill skapa affärer och det bygger på trust. Våra jurister är väldigt nitiska och vill hålla det väldigt snävt och det hämmar vår produktivitet i de vill göra med att bygga nya produkter och erbjuden. (Appendix B, #37).

Vi insåg dock i efterhand att flera större utlåtanden kunde innehålla flera färger. Detta ledde till att de transkriberade materialet som är bifogat i Appendix B, C och D blev väldigt svårläst och vi kunde inte heller presentera färgerna på ett tydligt sätt bredvid meningsinnehållet. Av den anledningen valde vi att lägga till bokstavskoder för att bibehålla spårbarheten men samtidigt öka läsbarheten av det transkriberade materialet. Bokstavskoderna är presenterade i kolumnen höger om färgerna i Tabell 6: **Kodningsmall** och är de som representerar våra områden i Appendix B, C och D.

Tabell 6: Kodningsmall

Område	Färg	Kod
Proactive not Reactive; Preventative not Remedial		PR
Privacy Embedded into Design		PED
Full Functionality – Positive-Sum, not Zero-Sum		FF
End-to-End Security – Lifecycle Protection		EES
Utmaningar		UT
Möjligheter/motivering		MM
Lösningar & andra tillvägagångssätt		ALH
Begreppet “Privacy”		BP
Övrigt		ÖVT

3.6 Undersökningskvalitet

För att säkerställa att den kvalitativa studien man genomfört är giltigt och går att lita på, är det viktigt kritiskt granska de slutsatser och empiriska material som innehas (Jacobsen, 2002).

3.6.1 Reliabilitet

Att granska reliabiliteten eller tillförlitligheten som det kan kallas, hos en uppsats innebär egentligen att man frågar sig: Kan jag lita på det här (Jacobsen, 2002)? Enligt Jacobsen (2002) kan ett antal faktorer påverka tillförlitligheten i en uppsats. Först ut är vad som kan kallas undersökareffekten som i sin tur består av två liknande fenomen men i olika datainsamlingsmetoder. Eftersom vi använt oss av intervjuer som datainsamlingsmetod ser vi till *intervjuareffekten*. Kort sagt innebär intervjuareffekten att intervjuaren själv kan påverka intervjuns stil och innehåll genom bland annat utseende, klädsel och hur man talar (Jacobsen, 2002). För att undvika att vi själva påverkade den som blev intervjuad försökte vi som

intervjuare vara så neutrala och konsekventa vi kunde i både utseende och tal. Eftersom vi använde oss av videointervjuer på distans var det bara vår överkropp som syntes i kameran, vilket gjorde det enkelt för oss att använda samma tröja under varje intervju. Vi gjorde också vårt bäst för att hålla intervjufrågornas formulering så lika som möjligt mellan intervjuer.

Enligt Jacobsen (2002) spelar också kontexten för intervjun roll. Alltså om den är artificiell eller naturlig för den som blir intervjuad. En artificiell kontext är helt enkelt en intervju som tar plats i en miljö som inte är familjär för den som blir intervjuad (Jacobsen, 2002). Eftersom vi nyttjade videointervjuer på distans utfördes intervjuerna i en miljö som intervjusubjektet alltid valde själv och som var naturligt för denne.

Slarv eller otillfredsställande analys av den empiriska data som samlats in, beskrivs också som en faktor till bristande tillförlitlighet (Jacobsen, 2002). Som tidigare nämnt valde vi att koda det transkriberade materialet separat för att på så sätt kunna korskontrollera varandras kodning och säkerställa att analysen förblev tillförlitlig. Transkriberingarna har också placerats i tabeller med meningsnummer, namn på talande person, meningsinnehåll samt koderna för den aktuella meningen. Detta gjorde vi för att öka spårbarheten av det empiriska resultatet vi presenterat och i förlängningen öka tillförlitligheten på vår studie.

3.6.2 Validitet

Validitet kan delas in två underkategorier: intern validitet och extern validitet (Jacobsen, 2002). Den interna validiteten syftar till att säkerställa att det insamlade empiriska materialet är vad som avsågs samlas in (att det är giltigt). Den externa validiteten i sin tur handlar om möjligheten att föra över det som funnits till andra sammanhang (att generalisera) (Jacobsen, 2002). För att uppnå både intern och extern validitet grundade vi vår undersökning på den litteratur vi gått igenom inom områdena integritet, Privacy by Design samt dataskyddsrätt. Som vi beskrivit tidigare var litteraturen väletablerad och ofta citerad av andra forskare på områdena. Litteraturen låg också till grund för den intervjuguide vi utformade. Vidare fokuserade vi mycket på att välja ut och finna rätt intervjupersoner. Som vi tidigare redogjort för ansåg vi att personerna behövde vara kunniga inom integritetsfrågor. De behövde besitta en relativt hög hierarkisk position i sin verksamhet samt att de själva varit delaktiga i integritets relaterade arbeten. Vi gjorde det tydligt för intervjupersonerna att vi inte avsåg att bedöma deras efterlevnad av olika legala krav. Vi ställde därför inte explicit frågor om de tre principerna från PbD som vi anser tydligt korrelerade med Dataskyddsförordningen. Vi gjorde detta för att minimera risken för att intervjupersonerna skulle känna sig ”klämda” och då eventuellt ge oss felaktig information.

Tyvärr hade vi inte möjlighet att genomföra fler än tre intervjuer vilket har en påverkan på både vår interna validitet och den externa. Många av de individer vi ansåg passade för vår undersökning valde att neka medverkan på grund av till exempel tidsbrist eller ointresse. Av de individer vi fick svar ifrån var vi också tvungna att välja bort en stor del eftersom vi ansåg att de inte mötte de krav vi hade på dem som intervjusubjekt. Det kunde då röra sig om bristande kunskap relaterat till integritet eller att de inte hade en tillräckligt bred organisatorisk vy (helikopterperspektiv). På grund av detta bör läsare av denna uppsats inte se resultatet som mer än indikationer eller övergripande beskrivningar av fenomen.

3.7 Etik

Etiska dilemman kan i flera fall uppstå i förhållandet mellan forskare och undersökande (Jacobsen, 2017). Dessa kan vara mer eller mindre allvarliga där de mest allvarliga är de som uppstår då undersökningen man utför fysiskt eller psykiskt kan skada andra människor (Jacobsen, 2017). När det handlar om etiska dilemman finns det inte några entydiga svar utan svaren man kommer fram till handlar snarare om den etiska utgångspunkt man som forskare väljer (Jacobsen, 2017). Det är viktigt att komma ihåg att det är fullt möjligt att genomföra en studie som är laglig men inte nödvändigtvis etiskt korrekt (Oates, 2006).

Till dagens forskningsetik finns det åtminstone tre grundläggande krav som kan användas som utgångspunkt (Jacobson 2017, 2002). Dessa tre krav som Jacobsen (2002, 2017) presenterar samt deltagarnas rättigheter enligt Oates (2006) har legat till grund för denna studies etiska utgångspunkt. Kraven korrelerar enligt vår uppfattning väl med varandra.

Informerat samtycke
Den som deltar i undersökningen ska frivilligt delta i undersökningen (Oates, 2006; Jacobsen, 2002) och en förutsättning för detta är att den undersökta är medveten om vilka risker och vinster som deltagandet eventuellt kan medföra (Jacobsen, 2002). I praktiken är det svårt att ge eventuella uppgiftslämnare tillräckligt med information om studien. Man skulle helt enkelt utsätta dem för informationsuttröttning (tar inte emot informationen) och det kan även leda till negativa konsekvenser för undersökningens tillförlitlighet. Om respondenten vet allt om vad studien syftar till, ökar det sannolikheten för att respondenten anpassar sina svar och inte återspeglar hur det egentligen ser ut (Jacobsen, 2002). Enligt Jacobsen (2002) behöver man således komma fram till vad som kan kallas ”tillräcklig information”. Denna bör innehålla uppgifter om studiens huvudsakliga syfte och om hur resultaten ska användas (Jacobsen, 2002).

Krav på privatliv
En avvägning av hur känslig den information som den undersökte lämnar ska alltid göras. Om informationen kan uppfattas vara känslig måste man lägga mer vikt i att garantera den undersöktes privatliv (Jacobsen, 2002). Risken uppstår framför allt när det finns möjlighet för utomstående att identifiera enskilda personer i datamaterialet för studien (Jacobsen, 2002). Är urvalet mindre, ökar risken för identifiering och därför är detta ett större problem i kvalitativa studier (Jacobsen, 2002). Finns det risk för identifikation kan man behöva överväga att vidta åtgärder för att försöka anonymisera data när de presenteras (Jacobsen, 2002). Två exempel på sådana anonymiseringsåtgärder som vi har använt är:

- Eliminering av data som kan bidra till identifikation av individer, dvs uppgifter om exempelvis ålder och kön.

- Låg detaljeringsgrad på data, exempelvis inte redogöra för exakt bakgrund för intervjusubjektet utan snarare benämna det som exempelvis ”lång arbetslivserfarenhet”.

Viktigt att poängtera här är även att organisationers identiteter bör vara anonymiserade/dolda såvida det inte är så att man får tillåtelse att använda deras namn (Oates, 2006).

Krav att bli korrekt återgiven

Analys av data innebär en reduktion av detaljer och mångfald. En fullständig återgivning är ett ideal men dessvärre någonting som aldrig helt går att uppnå. Resultatet från intervjun ska däremot i den mån det är möjligt återges i fullständigt och korrekt sammanhang (Jacobsen, 2002).

Tillvägagångssätt

Inledningsvis hörde vi artigt av oss till personer som vi förmodade uppfylla de kriterier som vi ställt för urval av intervjusubjekt. Kontakten tog vi via email och LinkedIn och meddelandet innehöll en kort presentation om oss och studien, studiens syfte, information om anonymisering samt intervjuns upplägg. Längst ner i meddelandet la vi även in en förklaring om vad det är för personer vi söker tillsammans med en vänlig uppmaning om att de gärna får hjälpa oss vidare i sökandet om dem känner att det finns bättre lämpade personer inom deras organisation eller kontaktnät.

Efter att ha fått positiv respons från potentiella intervjusubjekt kom vi överens om en tid som passade oss båda fint, därefter skickade vi ut en inbjudan till ett schemalagt Zoom-samtal samt intervjuguiden för att ge intervjusubjektet en möjlighet att bilda sig en uppfattning om frågornas karaktär.

Intervjuernas genomförande inleddes med en presentation av vem vi är, forskningsfrågan samt syftet med studien. Detta för att repetera och säkerställa att intervjusubjektet har tolkat tidigare information som vi delgivit dem i text korrekt samt ge subjektet möjlighet att ställa eventuella frågor som kan ha uppkommit. Innan själva intervjun påbörjades frågade vi om samtycke till inspelning samt om subjektet var okej med att spela in både röst och video eftersom detta, som tidigare nämnt, har varit optimalt för intervjuerna. En inspelning av intervjuerna ansåg vi vara ett krav för att ha möjlighet att senare transkribera materialet och på ett korrekt sätt återge vad subjektet sagt i intervjun. Vi erbjöd även intervjusubjektet att senare ta del av transkriberingen för att eventuellt korrigera fel och missuppfattningar alternativt be oss att utlämna delar av intervjun som de inte ville att vi skulle ha med i studien. Två utav intervjusubjekten önskade att vi skickade transkriberingen till dem men ingen utav dem ville ändra på eller förtydliga någonting.

Slutligen informerade vi en gång till om att vi har valt att anonymisera subjektet samt försäkrade subjektet om att materialet som vi samlar in endast kommer att användas för denna studie. Information om att det är helt okej att avbryta både intervju och medverkan i studien lämnades även innan vi påbörjade inspelningen och själva intervjun.

Den data som vi samlat in anser vi är av mindre känslig karaktär för individen då den snarare handlar om organisation än person. Vi har däremot ändå valt att anonymisera både organisation och person då insamlad data, ur ett organisationsperspektiv kan uppfattas vara betydligt mer känslig. En eliminering av data som kan bidra till identifikation av individer har senare gjorts i transkriberingsarbetet eftersom urvalet av respondenter är så pass litet och det därmed finns stor risk för identifikation.

4 Empiriska resultat

I det här avsnittet kommer vi presentera resultaten av vår empiriska undersökning. Svaren är indelade efter samma koder som beskrevs i kapitel 3, specifikt i Tabell 6: ***Kodningsmall****. Transkriberingar återfinns i Appendix B-D.*

4.1 Begreppet "Privacy"

IS1 inleder med att säga att hen förknippar privacy med begreppet integritet. IS1 beskriver hur de på Banken arbetar mycket med åtkomstkontroll och att de finner det viktigt att endast de personer som ska ha behörighet att komma åt data, ska kunna göra det. Mot kunderna säger IS1 att det är viktigt att skapa en känsla av trygghet och att de endast hanterar den data de sagt att de ska hantera.

Privacy för IS2 är tätt förankrat med vilken data som andra har tillgängligt om dig som person. IS2 talar om en transparens kring hur information om dig används och menar att privacy även handlar om vilka val man gör och möjligheten att ha ett val överhuvudtaget angående hur du vill att din egen data ska behandlas.

> Vad andra vet om dig, vad de samlar in om dig och i vilket syfte det sen används. Mot eller för din skull (Appendix C, #6).

IS3 säger att privacy är ett väldigt brett begrepp och väljer att särskilja begreppet till sitt privatliv och yrkesliv. När IS3 talar om begreppet i sitt privatliv är synsättet likt IS1 och IS2. IS3 utgår däremot i stället från sitt eget perspektiv och inte kundernas och säger att det då handlar om att säkerställa att hens uppgifter inte finns överallt. I yrkeslivet är IS3 som frilansare antingen involverad i ett utvecklingsarbete eller ett ledningsarbete ute hos sina kunder. I denna roll handlar begreppet mer om att säkerställa kompetensen i de team som IS3 sätter ihop så att lagringen sker på ett lagligt men även etiskt korrekt sätt.

> Men det primära syftet eller primära liksom syn på privacy för mig är att säkerställa att vi har ett utvecklingsteam som har kompetens på det, så att vi har en kompetensspridning på det när vi bygger saker, hur vi lagrar data, var vi lagrar data, hur vi använder den datan, att det görs på ett framför allt lagligt sätt men också på ett etiskt sätt liksom (Appendix D, #2).

Både IS1 och IS3 beskriver säkerhetsprocesser de använder i sina respektive verksamheter. IS1 redogör för hur Banken anlitat fler personer som arbetar med säkerhet som sin främsta uppgift men också att de tar in en extern firma för att granska deras kod och sedan försöka ”knäcka” den. IS3 berättar inte vem som utför arbetet men säger att det regelbundet förekommer pen-tester (penetration tests).

4.2 Proactive not Reactive; Preventive not Remedial

Två av våra intervjupersoner berättar att det finns ett tydligt engagemang från ledningen på respektive företag. IS1 motiverar engagemangen genom att säga att ledningen är ” … personligt ansvariga …” (Appendix B, #19). IS2 beskriver i stället att ledningens engagemang på Ad-tech-bolaget, härstammar från personliga värderingar som funnits sedan start. Dessa värderingar har dessutom, enligt IS2, lett till andra beslut angående integritet som varit strategiskt centrala för verksamheten. IS2 säger:

> Frånvaron av personlig data har ju blivit strategiskt central i hela organisationen, den påverkar allt vi gör idag så därför så är det ju det som vår marknadsavdelning skriver om, det är vad vår VD kommunicerar, det är vad jag som produktchef implementerar och för säljarna så är det de som dem är ute och säljer in till annonsörer och publicister (Appendix C, #14).

På frågor om företagskultur i relation till privacy redogör samtliga intervjupersoner för sin uppfattning. IS1 menar på att Banken har en företagskultur som involverar integritet men att den inte kommit förrän på senare år och att den till viss del fortfarande är under implementation. Ad-tech-bolaget har i stället en djuprotad relation till integritet enligt IS2. IS2 säger att det framför allt på utvecklarsidan när bolaget bildades, fanns personer som var engagerade i integritetsfrågor eftersom integritet ofta missbrukades i ad-tech industrin tidigare.

Eftersom IS3 är frilansande IT-konsult kan hen inte redogöra för företagskulturen i sitt eget bolag, utan ser i stället till de kunder hen jobbat för. IS3 menar på att det ofta finns en tydlig företagskultur som inkluderar integritet och att det ofta finns ett centralt ansvar för integritetsfrågor.

IS1 berättar att Banken har ett IT-arkitektforum där de granskar och bedömer tekniska lösningar innan de går ut i produktionsmiljö. Processen är enligt IS1, ”strömlinjeformat” (Appendix B, #25), vilket innebär att om de anställda följer de regler som finns uppsatta går det fort att gå igenom processen. För Ad-tech-bolaget är det inte lika strukturerat. IS2 säger att de är ”notorisk dåliga” (Appendix C, #16) när det kommer till dokumentation och formella processer. IS2 menar dock att detta kan bero på att de fortfarande har väldigt starka start-up rötter. I stället menar IS2 att de alltid har som utgångspunkt att bara samla in det dem kan stå för (dataminimering), vilket gör hela processen enklare. IS3 beskriver ungefär samma sak och menar på att de inte heller har några etablerade processer, utan att man snarare tar en extra fundering när det handlar om personuppgifter. IS3 säger också; ”Att säkerställa att vi bygger kvalitativa saker och att det innefattar att vi hanterar integritet, att vi hanterar personuppgifter på rätt sätt, det är liksom som en base-level för oss” (Appendix D, #12).

4.3 Privacy Embedded into Design

Som vi tidigare redogjort för menar IS1 att deras integritetsarbete blivit bättre under de senaste åren. Banken har idag mycket mer riktlinjer som styr agerandet. IS1 berättar om ett protokoll som de går igenom varje gång en ny tjänst eller produkt ska utvecklas. Utifrån denna klassificeras produkten där de tittar på om den innehåller någon form av persondata. Gör den det hanteras produkten på ett annat sätt.

En annan faktor som IS1 lyfter är den mänskliga faktorn.

> ... vi är ju människor och, ibland är vi kanske dåliga på att informera nya utvecklare om att; du kan inte logga personnummer här, du får inte, men så kommer det ändå ut där (Appendix B, #12).

För att stötta upp denna mänskliga faktor berättar IS1 om vissa ”smarta” komponenter som utvecklarna hos Banken använder sig utav. Dessa är menade att upptäcka känslig data och maska den i utvecklingsarbete. Det finns alltså en typ av skyddsnät hos Banken för att rädda upp vissa oönskade situationer.

Ad-Tech-bolaget (IS2) har inga formella processer eller metoder för att hantera integritetsbeslut utan har istället vissa grundprinciper som alltid grundar sig i vilken typ av data som de tänkt samla in. Detta är det helt centrala konceptet som Ad-tech-bolaget följer. När Ad-tech-bolaget vill gå i en viss riktning eller ser ett problem som de tror att de kan lösa bättre än en konkurrerande verksamhet menar IS2 att de alltid tvingas att tänka:

> Okej, vilken data kommer vi behöva för att kunna genomföra detta och faller det inom ramen för personlig data och att vi på något sätt behöver följa en användare i deras aktivitet på nätet, så går det bort. Då är det en sak som vi inte kan lösa det på det sättet, vi måste kika på andra sätt (Appendix C, #34).

IS3 har inte heller några formella processer för att exempelvis hantera dåliga integritetsbeslut utan har snarare en ansats som liknar Ad-tech-bolaget och IS2. IS3 menar att det finns med i tänket och är en del av kvalitetssäkringen nu för tiden.

> Inga bestämda eller etablerade processer utan det är bara att det är mer eller mindre underförstått, i alla fall i dem teamen som jag jobbat med att så fort det handlar om personuppgifter då tar man en extra fundering, framför allt när vi diskuterar arkitektur och design ... så det finns ju absolut med i tänket, det är en del av att bygga ett system som har liksom, det är en del av kvalitetssäkringen nu för tiden, i alla fall i mina team (Appendix D, #12).

4.4 Full Functionality – Positive-Sum, not Zero-Sum

På frågor om integritetsarbete hämmar eller försvårar framtagandet av produkter eller tjänster fick vi delade svar från våra intervjupersoner. IS2 och IS3 menar att det inte hämmar framtagandet, utan att det snarare förenklar det. IS2 menar att integritet gör att de tänker annorlunda kring tekniska utmaningar. IS2 säger:

> Så någonstans så har det blivit så att vårt privacy-arbete de informerar våra tekniska utmaningar snarare än tvärtom. Vi innoverar och kommer med nya typer av lösningar i och med vårt privacy-arbete och summa summarum så ska jag säga att vi blir en snabbare organisation och snabbare tekniskt för det finns väldigt många frågor som vi inte behöver hantera … (Appendix C, #26).

IS2 poängterar också att Ad-tech-bolaget har som grundpelare att inte samla in personuppgifter överhuvudtaget. Detta innebär, enligt IS2, att de hela tiden måste kontrollera och se över så att de inte oavsiktligt samlar in personuppgifter.

IS3 beskriver en likande förenkling och berättar att det till viss del gör arbetet enklare eftersom de måste använda sig av standardiserade lösningar för till exempel inloggning. IS3 fortsätter och säger att det innebär att valmöjligheterna minskat men att det måste implementeras för att göra de säkrast möjliga valen för användarna.

IS1 är mer delad i sitt svar. När vi direkt frågar om integritetsarbetet förhindrar eller hämmar utvecklingen av produkter eller tjänster, svara IS1 att det inte gör det om man anammar de regler som finns på Banken. I andra utlägg säger IS1 dock att Bankens jurister har en väldigt snäv och nitisk tolkning av legala krav. IS1 säger ” … det hämmar vår produktivitet i de vill göra med att bygga nya produkter och erbjuden” (Appendix B, #37) och ”Det är det jag menar med att vi är väldigt snäva i vår tolkning vilket gör att vi hämmas av att kunna nyttja ny cool teknik som faktiskt skulle förbättra oss och göra oss ännu bättre” (Appendix B, #41).

När det kommer till hur organisationerna prioriterar integritetsfrågor är svaren återigen delad. IS1 säger att på Banken kommer affären först, även om integritet väger väldigt tungt för vissa anställda. IS3 säger att hos hens kunder är det snarare så att man inte får prioritera bort integritet och om man gör det kan det få stora konsekvenser. IS2 säger däremot att på Ad-tech-bolaget prioriterar man integritet över de tekniska målen.

4.5 End-to-End Security – Lifecycle Protection

Organisationerna och intervjusubjekten som vi intervjuat har olika sätt att arbeta med integritetsfrågor genom produkters livscykler. Det verkar däremot inte finnas några strukturerade processer för denna typ av arbete hos någon av verksamheterna men samtliga utrycker att arbetet sker.

Enligt IS1 är det störst fokus hos Banken då de ska sätta något nytt i produktion. IS1 menar däremot att Banken är rätt bra på att uppmärksamma om det kommer nya regler som de måste anpassa sina produkter efter och implementera. I dessa fall så är det ofta avdelningarna för ”legal” och ”security” som ger input, ansvaret att identifiera dessa eventuella justeringar som kan behöva göras ligger alltså snarare här än hos utvecklarna.

En annan åtgärd som IS1 lyfter är deras loggar. Idag säger IS1 att detta är uppstyrt så att anställda har tillgång till de loggar som de ska ha tillgång till och inte alla såsom det tidgare varit.

> En sak om det här med loggarna, tidigare så hade alla tillgång till loggar och det är nu helt uppstyrt så du får tillgång till de loggarna som du ska ha tillgång till. Är du ansvarig för en tjänst då är det klart att du får gå in och titta i loggarna för den, men är du inte det då får du fråga den som är ansvarig som får ta fram uppgifterna åt dig om det anses lämpligt (Appendix B, #39).

Hos Ad-tech-bolaget är det, som tidigare nämnt, alltid dataminimeringen som ligger till grund för deras arbete och det är enligt IS2 således denna som dem hela tiden måste hålla koll på.

> Du behöver inte ha så mycket processer kring att kontrollera att utrensningen har funkat som den, alltså: rensa upp i dina loggar, rensa upp i databaser, rensa upp i back-ups osv,

> för att du vet att ditt dataset innehåller inte personlig känslig information (Appendix C, #26).

IS3 säger att det absolut har blivit ett större fokus på att tänka på privacy i varje steg av utvecklingen. IS3 säger att data exempelvis ska rensas med jämna mellanrum och att det finns kontroller på den typen av åtgärder. Eftersom IS3 lämnar ifrån sig produkterna för förvaltning till kunderna, så går hen däremot inte in djupare på hur detta arbete sker eller vilka processer som finns här.

4.6 Utmaningar

Banken och IS1 har ett samarbete med jurister. IS1 säger: ”Vi samarbetar men vi har helt olika synsätt på saker och ting” (Appendix B, #41), och ”men som sagt vi har olika synsätt på risk och trust” (Appendix B, #41). IS1 nämner ny teknik såsom molnet som ett exempel där synsättet mellan jurister och analysavdelningen (i detta fall) kan skilja sig.

> Här brottas vi just nu med att utbilda och lärare om vad det innebär att ha data i molnet som är väldigt på tapeten (Appendix B, #41).

En annan utmaning som IS1 tar upp är språket och kommunikationen, både vad det gäller legala krav och privacy by design som ansats. På frågan om begreppet PbD används i organisationen säger IS1:

> Man kan säga så här, jag tror inte att alla känner till det och vi har haft den här approachen att mer utbilda, informera. Där använder vi inte direkt Privacy by Design men vi pratar i de termerna. Så kan jag säga. Om vi pratar med säkerhet och dem, Ja, då är det Privacy by Design. Visst språk fungerar inte på alla. Vi vill hålla det så enkelt som möjligt för våra utvecklare egentligen, och då är det “ni ska inte logga username, password”, “ni ska inte logga kreditkortsnummer med expiry date” och så vidare. Vi pratar mer i dem termerna där (Appendix B, #14).

När det kommer till legala krav och hur dessa förmedlas till utvecklarna säger IS1 att ”en lagtext är kanske inte för alla att läsa” (Appendix B, #18) och berättar hur hen arbetat för att få fram en ”översättning” av exempelvis GDPR till vad IS1 benämner som ”utvecklar-språk”. Det har alltså skett ett samarbete med ”legal” där dem kommit fram till ett sätt att förmedla legala krav till utvecklare så att dem förstår språket.

IS1 har som tidigare även talat om den mänskliga faktorn och exemplifierar detta med att det har hänt att man inte har förstått allvaret i en produkt som borde ha tagits upp i det tidigare nämnda arkitekt-forumet. Det ska tilläggas att IS1 poängterar att detta har blivit avsevärt mycket bättre på senare tid och att det sällan händer idag.

> ... vi har ju upptäckt att det har kommit upp grejer som borde tagit upp i ett sådant här arkitektur-forum där vi godkänner grejer som har struntat i att berätta det. Man har inte förstått allvaret ... (Appendix B, #25).

IS1 lyfter även under intervjun att en av de svårare delarna av arbetet är att få anställda att följa givna regler, policys eller processer utan att de anställda upplever att de blir kontrollerade eller övervakade.

> Hur man får folk att följa det utan att agera polis, Det är ju det svåra. Det är jättesvårt vill jag påstå (Appendix B, #29).

Både IS1 och IS2 tar upp i intervjuerna att det som följd av ett gediget integritetsarbete kan vara svårt att se någon direkt vinst i form av pengar.

> Så visst, det hämmar ju vår utveckling för att vi lägger ju tid på saker som egentligen inte är en vinst för bolaget i form av pengar, alltså vi tjänar ju inga pengar för men i gengäld så vill ju vi vinna trust och det i sin tur kan ju ge pengar så det är en sidoeffekt av att vi är duktiga på detta (Appendix B, #19).

> För oss är utmaningen mer: hur tjänar vi pengar när vi går en helt annan riktning? Hur fortsätter vi vara konkurrenskraftiga med någonting som är så annorlunda? (Appendix C, #42).

IS3 diskuterar aldrig det monetära värdet av integritetsarbete, men tar upp andra utmaningar som är relaterade till integritetsåtaganden. På frågan; Kommer ni då med exempel på lösningar eller arbetar ni utefter deras policyers? Svarar IS3 att kundernas policyer ofta är lite lösare och att systemen IS3s team utvecklar tenderar att vara mer strikta i sin tolkning av integritetskrav. IS3 säger dock att om kunderna inte vill mottaga ett system med vad IS3 anser vara best practices relaterat till integritet så får de fråga sig själva: ”är vi villiga att leverera det här, men till någonting som vi anser är av sämre kvalitet?” (Appendix D, #32).

4.7 Möjligheter/motivering

På frågor om vad som motiverar intervjupersonernas verksamheter att arbeta med integritet svarar samtliga att det ofta relaterar till Dataskyddsförordningen. IS1 berättar att det kommer anonyma kontroller ett par gånger om året för att se till så att Banken sköter sig och att de följer de regler och lagar som finns på området. IS1 berättar också att det för dem handlar mycket om tillit och trovärdighet. Hen menar på att tilliten de får från sina kunder i sin tur kan leda till att de tjänar mer pengar men också att de kan få utstå mycket badwill om de skulle missbruka kundernas förtroende.

> Skulle vi då komma fram till att någon kommer att granska oss och hitta det här: alltså varför sparar ni alla kunders transaktioner på deras utgifter, ni skulle bara ta hand om deras inkomster. Då kommer det stå någonstans och det kommer bli en otrolig badwill. Hamnar du på förstasidan på Aftonbladet, den badwillen är så dyr så att vi inte tar den risken helt enkelt. Detta är tok viktigt vill jag påstå (Appendix B, #37).

IS2 redogör också för hur Dataskyddsförordningen påverkade Ad-tech-bolaget. Hen säger att det var först när GDPR trädde i kraft som verksamheter hade något att förhålla sig mot och efterleva. IS2 säger också att det var speciellt tydligt i deras bransch då den låg så otroligt långt ifrån de lagar som började gälla. Det var alltså i denna omställning Ad-tech-bolaget valde att släppa allt som hade med persondata att göra. IS2 menar att det för Ad-tech-bolaget skulle varit svårt att inhämta ett informerat samtycke och att det dessutom inte skulle legat i användarnas intresse att lämna ett sådant. Genom denna omställning beskriver IS2 att ad-tech-bolaget också skapat en väldig trygghet för dem själva men också deras kunder. Eftersom de inte samlar in persondata så utsätter de inte någon för risken att få böter i framtiden.

IS3 är inne på samma spår och säger att alla bolag fick genomgå en självgranskning i samband med att Dataskyddsförordningen började gälla. På frågan om varför hen arbetar med integritetsfrågor inleder hen skämtsamt och fortsätter sedan säga:

> Varför? för att våra kunder inte vill bli stämda och böta. Nej, Nej det är inte alls så utan generellt sätt så tycker jag att folk har vaknat till av hur data säljs och det är i tiden och därför så får man säkerställa att man behandlar data på ett sätt som är etiskt och schysst mot ens användare precis som att man själv hade velat att bolag gör med ens egna data helt enkelt (Appendix D, #8).

IS3 tillägger också:

> Jag tror bara att det är mer och mer medvetet, det handlar inte lika mycket nu längre i dialogen om att "vi ska inte bli stämda, vi ska inte få böta" utan nu handlar det mer om att "Vad är rätt för användarna och vad behöver vi egentligen ha för data? Det finns inget syfte att vi ska ha tre emailadresser, hemadress plus målsmans samtliga uppgifter också, vi kanske kan nöja oss med det enklaste liksom (Appendix D, #8).

IS3 berättar också att som frilansande IT-konsult så kan det finnas andra anledningar att arbeta med integritet. IS3 säger att det för honom kan vara en form av kvalitetsstämpel som är användbar både för att bygga upp sitt varumärke men också för att locka till sig och behålla bra konsulter. IS3 menar på att kunder uppskattar när hen tagit ansvaret för att säkra integritet vid utvecklingen av diverse IT-artefakter, eftersom det i slutändan är kunderna som ansvarar för systemen.

4.8 Lösningar & andra tillvägagångssätt

Språket och kommunikationen är som tidigare nämnt en av utmaningarna hos Banken. För att lösa denna problematik har Banken tillsammans med sina jurister försökt att plocka fram en typ av översättning av legala krav såsom GDPR, som är menad att vara mer mottagbar av utvecklarna.

> Ja, vi tog och skrev utkastet och sen så har vi visat det och fått godkänt på att "ja men så här kan man också uttrycka sig" En lagtext är kanske inte för alla att läsa. Jag vill att man ska kunna uttrycka dem enklare men innebörden ska ändå vara densamma såklart (Appendix B, #18).

Utbildningar av olika slag har förekommit i våra intervjuer. IS1 berättar i sin intervju hur de på Banken har obligatoriska utbildningar för alla anställda där integritetsfrågor inkluderas. Hen poängterar dock att hen gärna hade velat se specifika integritetsutbildningar för utvecklare, eftersom hen upplever att det är väldigt viktigt.

På Banken berättar IS1 att de också arbetar med olika tekniska hjälpmedel för att säkra implementationen av integritet. Hen beskriver hur de framför allt kämpar för att automatisera så mycket så möjligt. Hen nämner specifikt att de automatiskt "maskar" kunddata även om det hade varit ok enligt lag att göra det manuellt.

5 Diskussion

I det femte kapitlet ställer vi vårt empiriska resultat mot den forskning vi presenterat i kapitel 2. Vi kommer belysa skillnader, likheter och andra relevanta aspekter med vår empiri i förhållande till den tidigare forskning vi presenterat.

5.1 Synen på begreppet "Privacy"

5.1.1 Privacy

Begreppet privacy är tvetydigt och det kan resultera i att begreppet tolkas olika beroende på i vilken kontext som det presenteras. I våra intervjupersoners fall är frågan om hur de ser på begreppet privacy ställd i en kontext då de suttit i sina respektive yrkesroller. Hade frågan ställts till intervjupersonerna i exempelvis en privat kontext hade svaren kunnat se annorlunda ut. IS3 är den enda som tydligt väljer att dela upp begreppet till privat och yrkesliv i stället för att hålla ett generellt perspektiv.

IS1 förknippar begreppet hårt med den vanligt förekommande översättningen till det svenska språket, integritet. Den traditionella betydelsen enligt Kroener och Wright (2014) om att rätten till privacy skulle vara en sorts rätt att bli lämnad ifred (översatt) stämmer väl överens med hur IS2 väljer att se på begreppet då hen säger att det även handlar om ”möjligheten att ha ett val överhuvudtaget kring hur du vill att din egen data ska behandlas” (Appendix C, #6).

Kroener och Wright (2014) poängterat att begreppet bör betraktas i förhållande till lagstiftningsdefinitioner. GDPR talar snarare om rätten till skydd av personuppgifter än integritet. Det är tydligt att samtliga intervjupersoner talar om en rätt att få sina personuppgifter skyddade. Det går därför att argumentera för att intervjusubjekten ser på begreppet i ljuset av de legala krav som idag är gällande, men värt att tillägga är att begreppet är brett, vilket även IS3 poängterar i sin intervju.

5.1.2 Privacy vs Security

Under intervjuerna förekom det fall när intervjupersonen benämnde integritet som säkerhet eller använde begreppen synonymt. På frågan om integritet prioriteras på samma sätt som andra design- eller innovationsmål svarade IS1 att de anlitat flera personer under de seanste 4 åren som bara jobbar med säkerhet. Hen beskrev också hur de anlitar en extern firma som kontrollerar och försöker knäcka deras kod. IS3 beskrev ett liknande scenario men sade att de utförde ”pen-tester” även kallat penetration tests. Denna förväxling av begreppen stämmer väl överens med vad Spiekermann (2012) säger och hon tillägger även att det är viktigt att organisationer förstår vad de faktisk försöker skydda. Kroener och Wright (2014) menar att förväxlingen kan orsaka problem på framförallt två fronter. Om begreppen ses som synonyma är det troligt att det finns en avsaknad av att tydligt veta vad organisationen försöker skydda. Detta kan i sin tur leda till att organisationer får det svårt att bedöma hur mycket medel de ska

allokera till bägge målen. Vidare kan det leda till en falsk trygghet där organisationer tror att de värnar om individers integritet, men i själva verket har de endast tekniska säkerhetsmekanismer på plats, vilket endast är en del av att värna om individers integritet enligt Privacy by Design.

5.2 Proactive not Reactive; Preventive not Remedial

Ansatsen PbD väntar inte på att personuppgiftsincidenter ska inträffa och erbjuder därmed inte några lösningar eller åtgärder för när ett integritetsarbete brister. Man ska arbeta proaktivt med integritetsarbetet så att bristerna inte uppkommer i första hand (Cavoukian, 2009).

Samtliga organisationer redogör för att det finns ett engagemang hos respektive ledning. Värt att notera är att IS3 som frilansare snarare ser detta engagemang hos kunderna som hen arbetar för. Enligt Cavoukian (2009) bör ledningen främja detta engagemang och andra integritetsåtaganden till övriga delar av organisationen för att skapa en företagskultur som speglar detta synsätt. IS2 och Ad-Tech-bolaget sticker ut i denna fråga då ledningens engagemang på Ad-tech-bolaget har sina grunder i personliga värderingar som funnits sedan start. Hos Ad-tech-bolaget är frånvaron av personlig data strategiskt central i hela organisationen. Detta talar för att det finns en högre nivå av integritet hos Ad-tech-bolaget än vad lagar och andra juridiska krav kräver. Viktigt att poängtera här är att alla affärsmodeller kanske inte är kompatibla med detta tillvägagångssätt. Att helt eliminera all persondata hade exempelvis inte varit möjligt för Banken.

IS2 redogör för hur organisationen inför att GDPR skulle träda i kraft landade i det strategiska beslutet om att släppa all personlig data och istället arbeta helt kontextuellt. IS1 säger att Banken har en företagskultur som involverar integritet men att den inte kommit förrän på senare år och att den till viss del fortfarande implementeras. Man kan tolka detta som att engagemanget och kulturen kring integritetsfrågor är någonting som snabbare vuxit fram på senare tid, inte minst i samband med att GDPR trädde i kraft år 2018.

För att korrigera eventuella negativa effekter innan de inträffar menar Couvakian (2009) att organisationer bör anamma metoder för att identifiera dåliga integritetsstandarder. Både IS2 och IS3 redogör för att de inte har någon direkt dokumentation eller formella processer för att hantera integritetsbeslut. IS2 och Ad-tech-bolaget har istället alltid som utgångspunkt att bara samla in det de kan stå för (dataminimering), vilket IS2 argumenterar för gör denna process enklare. IS3 säger att man snarare tar en extra fundering när det handlar om personuppgifter, att hantera personuppgifter korrekt är ”*base-level”* för IS3:s team. IS1 och Banken har däremot något mer formella processer och metoder för att hantera integritetsbesluten. De har bland annat tekniska hjälpmedel som ska användas av utvecklare men även ett IT-arkitektforum där de granskar och bedömer tekniska lösningar innan de går ut i produktionsmiljö. Både Ad-tech-bolaget och IS3s verksamhet är betydligt mindre organisationer än Banken. Detta kan vara en bidragande faktor till att man inte har prioriterat att ta fram denna typ av formella processer. Varken IS2 eller IS3 utrycker däremot att de saknar denna typ av formaliteter. IS2 berättar bland annat att de har kvar sina starka start-up rötter och menar att detta kan vara en bidragande faktor till att de inte satt sig ner och etablerat några formella processer. IS2 menar att det alltid är större fokus på andra saker som gör större skillnad direkt och nämner även att det är relativt lätt att sprida information i ett bolag som deras som fortfarande är relativt litet. Det finns enligt oss ett tydligt integritetsåtagande som

delas av användargrupper och intressenter hos bolagen även om engagemanget och processerna relaterat till integritet helt klart skiljer sig åt.

5.3 Privacy Embedded into Design

Två utav tre intervjupersoner beskriver att de inte följer några accepterade standarder eller ramverk när det kommer till implementeringen av integritet i olika IT-artefakter. I stället förlitar de sig på vad som närmst kan liknas med personliga värderingar eller kollektiv kunskap inom organisationerna. För att förtydliga är det viktigt att komma ihåg att Ad-tech-bolaget valt att utesluta all persondata och på så sätt uppnå den kanske högsta nivån av dataminimering. Av den anledningen behöver de inte heller följa samma standarder som till exempel den frilansande IT-konsulten. Hur organisationerna valt att behandla dessa punkter både möter och går emot hur Cavoukian (2009) säger att organisationer bör implementera integritet. Båda bolagen har ett systematiskt och principfast sätt att implementera integritet men det baseras inte på etablerade ramverk eller standarder. På grund av det kan inte heller externa parter med samma enkelhet granska bolagen i enlighet med PbD:s princip. Banken och IS1 redogör för ett mer formellt tillvägagångssätt med riktlinjer och protokoll men berättar inte vad de är baserade på.

Risk-och påverkansbedömningar ska genomföras så ofta de kan enligt PbD:s principer (Cavoukian, 2009). Kroener och Wright (2014) och Van Lieshout et al. (2011) instämmer med detta synsätt. Kroener och Wright (2014) skriver att Privacy Impact Assessments kan hjälpa organisationer att identifiera integritetsrisker och på så sätt veta var PbD bäst kan appliceras. Ingen av de organisationer som våra intervjupersoner arbetar för verkar arbeta med risk-och påverkansbedömningar på detta sätt. Ad-tech-bolaget är de enda som tydligt säger att de använder sig av riskbedömning vid hantering av integritetsfrågor. IS2 berättar att de regelbundet förekommer riskbedömningar tillsammans med deras kunder. Hen säger också att hen gärna hade velat se samma typ av återkommande riskbedömningar internt. IS1 talar också om risker men endast indirekt om riskbedömningar. Hen berättar om risker de inte är villiga att ta och hur synen skiljer sig internt inom verksamheten. På grund av det förutsätter vi att någon form av riskavvägning har gjorts även om det inte varit en grundlig riskbedömning. Även om Ad-tech-bolaget genomför sina riskbedömningar så redogjorde de inte för om resultaten av dem publiceras i enlighet med PbD.

5.4 Full Functionality – Positive-Sum, not Zero-Sum

PbD som ansats är väldigt mån om att inte påverka och försämra en produkt eller tjänst bara för att tillverkaren valt att värna om integritet. Den fjärde principen för PbD ämnar se till så att en tjänsts fulla funktionalitet bibehålls även vid integrering av integritet (Cavoukian, 2009). På samma sätt ska inte integritet heller behöva konkurrera med andra mål så som design- eller tekniska mål (Cavoukian, 2009).

Våra intervjupersoner var något delade i sina svar, även om de alla svarade att integritet inte hämmar eller försvårar framtagandet av tjänster och produkter. IS2 och IS3 svarade tydligt med att integritetsarbetet nästintill underlättade framställandet av en tjänst. IS2 går till och med så långt som att säga att de har blivit en snabbare organisation och att de är snabbare på teknisk utveckling, på grund av de integritetsval de tidigare gjort. IS3 säger att

integritetsarbete förenklar till viss del eftersom det kan tvinga dem att använda standardiserade tillvägagångssätt för till exempel inloggning. På så sätt minskar valmöjligheten och beslut kan fattas snabbare. Både IS2 och IS3 arbetar på ett sätt som stämmer väl överens med PbD-principens åtagande för att inte kompromissa med funktionalitet. IS1 däremot, redogör för en delad syn. På frågan: ”anser du att integritetsarbetet förhindrar eller hämmar framtagningen av produkter eller tjänster?” svarar hen att hen inte tycker den gör det om man följer de regler som finns på Banken. Senare i intervju säger hen dock att Bankens jurister har en snäv tolkning av legala krav på integritet, vilket hämmar dem (utvecklarna), på olika sätt. På grund av IS1s delade svar kan vi tolka situationen på Banken på olika sätt. Det kan vara så att IS1 inte alls anser att integritetsarbetet fungerar som det ska, men att hen inte vill säga det om sin arbetsgivare. Det kan också vara så att det fungerar bra för de idéer som blivit godkänna att gå till utveckling men att många idéer har fått skrotas på grund av juristernas snäva tolkning av till exempel Dataskyddsförordningen. Oavsett stämmer detta arbetssätt inte alls överens med PbD:s princip och det ger en indikation på att Bednar, Spiekermann och Langheinrichs (2019) slutsats om att jurister och systemutvecklare har svårt att komma överens, stämmer.

PbD:s fjärde principer ämnar också att likställa integritetsåtagande med andra legitima intressen, så som designmål och innovativa tekniska lösningar (Cavoukian, 2009). Intervjupersonerna redogör för tre tydliga nivåer av prioritet. IS1 säger att Banken prioriterar affärer framför integritet. IS3 säger att man inte kan prioritera bort integritet hos hens kunder. Slutligen säger IS2 att integritet är det som styr eller är överordnat alla andra legitima mål eller intressen. Hur den fjärde principen i PbD än tolkas är det tydligt att Bankens förhållningssätt inte stämmer överens med vad PbD avser. Hos IS3 och IS2 är det svårare att avgöra. Det kan till synes verka som att IS2 och Ad-tech-bolaget har den ”bästa” synen på integritet men det stämmer inte nödvändigtvis med PbD:s fjärde princip som menar på att integritet ska *likställas* med andra intressen. Integritet ska inte nödvändigtvis styra utvecklingen. IS3s synsätt går egentligen mer i linje med vår tolkning av vad PbD avser i denna princip. Eftersom IS3s förhållningssätt garanterar att integritet alltid behandlas eller finns med i utvecklingen, utan att det konkurrerar ut andra intressen.

5.5 End-to-End Security – Lifecycle Protection

Ingen av intervjupersonerna uttryckte något specifikt tillvägagångssätt för att monitorera integritet i hela produktens livscykel. Däremot menade samtliga att arbetet i någon mån sker. Stark åtkomstkontroll och loggning som Cavoukian (2009) förespråkar för att skydda personuppgifter kan man tydligt se hos IS1. IS2 menar snarare att de egentligen inte behöver ha några processer för att kontrollera att persondata är säker efter att en produkt eller tjänst har gått ut i produktion. Detta är återigen på grund av den dataminimering som Ad-tech-bolaget anammat och de behöver därför exempelvis inte rensa ut redundant eller irrelevant persondata.

Att följa en etablerad standard för att säkerställa integritet förespråkas av principen End-to-End Security (Cavoukian, 2009). Även om organisationerna menar att de tar ansvar för persondata genom hela produktens livscykel redogör de aldrig för någon standard som de följer.

5.6 Utmaningar

En av utmaningarna med Privacy by Design som Alshammari och Simpson (2017) skriver om, är avsaknaden av systematiska metoder för att hantera komplexiteten och variationen av integritetsproblem. Integritetsarbetet hos de olika organisationerna som vi intervjuat skiljer sig helt klart åt och tittar man exempelvis på IS1s och IS2s organisationer kan man se att de har helt olika utgångspunkt när det kommer till integritetsfrågor. Eftersom Ad-tech-bolaget och IS2 har som utgångspunkt att helt eliminera persondata lyckas de exempelvis komma runt en del av de legala krav som idag ställs på organisationer när det kommer till personuppgifter. Dessa legala krav (GDPR) används snarare som en utgångspunkt för IS1s och IS3s verksamheter. Även om IS2 och Ad-tech-bolaget inte förhåller sig till GDPR i samma utsträckning som exempelvis Banken och IS1 sker ett gediget integritetsarbete hos Ad-tech-bolaget. Frånvaron av personlig data är som IS2 berättar strategiskt central i hela organisationen och vi tolkar det som att detta även är en av de viktigare delarna av deras produkt.

Flera tidigare studier (Alshammari & Simpson, 2017; Bu et al., 2020; Chen & Williams, 2013; Gürses, Troncoso & Diaz, 2011; Spiekermann, 2012) har poängterat att många av utmaningarna med PbD främst ligger i transformeringen av PbD:s principer till faktiska implementerbara krav eller aktiviteter för systemutvecklarna. Som en följd av ovan nämnda komplexitet och variation av integritetsarbete skulle man kunna argumentera för att några universellt applicerbara krav och aktiviteter för systemutvecklare helt enkelt är svårt att utforma. Arbetet med att transformera PbD:s principer kanske, som en följd av PbD:s omfattande natur måste ligga på företagen själva att utforma. Något gediget arbete med att utforma denna typ av aktiviteter för systemutvecklare kan vi däremot inte direkt se hos någon av de organisationer som vi intervjuat. Dock påpekar Van Rest et al. (2014) att om varje organisation själva ska utforma sina lösningar, kan innovation främjas, men det kan komma till bekostad av transparens.

En annan utmaning som Bednar, Spiekermann och Langheinrich (2019) tar upp är svårigheterna med att få jurister och systemutvecklare att samarbeta i relation till de legala krav som finns för integritet. Denna utmaning återspeglas tydligt hos Banken och IS1 som talar om att juristerna och utvecklarna/ledningen har olika synsätt på ”risk” och ”trust” vilket IS1 menar i viss mån hämmar arbetet hos organisationen.

Som både IS1 och IS2 säger i sina respektive intervjuer kan det vara svårt att se ett penningvärde i ett bra integritetsarbete. IS1 säger att det snarare är den ”trust” man bygger upp hos kunderna som i sin tur kan genera pengar och hos IS2 kan man tolka det som att integritetsarbetet är en stor del av den produkt som de erbjuder. Det tycks alltså vara svårt att värdera ett gediget integritetsarbete.

5.7 Möjligheter/motivering

Organisationers möjligheter med integritetsåtagande är fortfarande relativt outforskat. Än så länge har det främst handlat om att undvika negativa konsekvenser om man inte arbetar med integritet. Cavoukian och Chibba (2018) säger dock att PbD kan öka tilliten kunder känner för en organisation. IS1 är inne på samma spår och motiverar deras arbete med framför allt skapandet av tillit hos sina kunder. Hen menar också att tilliten i förlängningen leder till fler affärer för Banken vilket är ett resonemang Cavoukian och Chibba (2018) delar. På samma

sätt beskriver IS1 den badwill som kan komma av att bryta förtroendet hos sina kunder. Hen menar att det skulle kosta Banken så mycket pengar att de helt enkelt inte vill ta den risken. Cavoukian och Chibba (2018) har samma synsätt men adderar att det även kan leda till förlorade marknadsandelar.

Ad-tech-bolaget som såg svårigheter med att samla in informerade samtycken valde istället för att ta risker, att totalt göra sig av med persondata och anamma dataminimering till sitt yttersta. Genom en total avsaknad av persondata så undgår Ad-tech-bolaget också de negativa konsekvenser som tidigare beskrivits när tillit bryts. IS2 beskrev också att branschen de befinner sig i tidigare var väldigt långt ifrån gällande lagar och regler. Ad-tech eller annonsbolag har varit kända för att samla in stora mängder data om sina användare eller besökare. Att Ad-tech-bolaget i fråga valde att göra sig av med all persondata kan varit speciellt viktigt för dem, eftersom dataläckor tenderar att öka i allvarlighet om företag är för beroende av persondata (Bu et al., 2020). Resultatet som IS2 beskriver, verkar också ligga i linje med vad Cavoukian, Taylor och Abrams (2010) skriver. IS2 berättar att hen upplever att Ad-tech-bolaget nu är en snabbare organisation och snabbare på att skapa nya tekniska lösningar eftersom de inte behöver ta lika många beslut om integritet.

Något som inte redogjordes för i tidigare litteratur vi läst var det faktum att integritet kan fungera som ytterligare ett sätt att bygga sitt varumärke för IT-konsulter. Precis som IS3 säger uppskattar hens kunder när hen tar ansvar för att implementera och efterleva de legala krav som finns på integritet. På så vis stärker hen sitt varumärke och får ytterligare ett argument att sälja in kunder på.

5.8 Lösningar & andra tillvägagångssätt

Precis som vi beskrev under rubriken 5.6 Utmaningar så har IS1s organisation, Banken, haft problem med att jurister och systemutvecklare har olika perspektiv och inte kan kommunicera på ett bra sätt. För att lösa en del av detta dilemma valde Banken att ta fram en omskrivning av Dataskyddslagen. Omskrivningen var skriven med ett språk som lämpade sig bättre för systemutvecklare. Detta kan vara ett sätt att implementera förslaget om att skapa förenklade och tydliga riktlinjer för utvecklare som Senarath och Arachchilage (2018) lade fram.

Senarath och Arachchilage (2018) diskuterar också utbildning som ett verktyg för utvecklare. De fann att utvecklares bristande kunskap, relaterad till integritet, hindrade de att effektivt implementera integritet i utvecklingen av system. IS1 berättar att de på Banken har utbildningar som innefattar integritet, men att utbildningarna inte är riktade till utvecklare specifikt. IS1 säger dock att hen själv hade velat se den typen av utbildning på Banken, eftersom hen upplever att det är en viktig fråga.

IS1 berättar också för oss att de nyttjar en del tekniska hjälpmedel för att hantera säkerställningen av integritet. Hen talar framför allt om att öka graden av automatisering så mycket som möjligt för att på så sätt minimera den mänskliga handpåläggningen och risken att människor gör fel. Det kan även leda till att insynen och tillgången till persondata blir mer begränsad. Användningen av sådana tekniska hjälpmedel förespråkas bland annat av Kroener & Wright (2014) i deras alternativa tillvägagångssätt.

6 Slutsats

Syftet med denna studie var att undersöka och beskriva hur personer i en ledande roll och deras organisationer arbetar med integritet i förhållande till ansatsen Privacy by Design. För att gör det svarade vi på forskningsfrågan: *Hur förhåller sig integritetsarbetet hos personer i en ledande roll och deras organisationer till ansatsen Privacy by Design?*

Privacy är ett brett begrepp. Vårt empiriska resultat visar att samtliga intervjupersoners resonemang av begreppet privacy mynnar ut i att individer har en rätt att få sina personuppgifter skyddade. Intervjupersonerna ser alltså begreppet i ljuset av de legala krav som idag är gällande, precis så som Kroener och Wright (2014) poängterat att man bör göra.

Vår studie styrker den komplexitet och variation av integritetsproblem som påvisats i tidigare forskning. Organisationerna som vi har intervjuat har inte samma utgångspunkt när det kommer till integritetsfrågor. De åtaganden som organisationerna väljer att ta i förhållande till integritet varierar således. Det ska tilläggas att de organisationer som vi intervjuat varierar i storlek. En mindre organisationen kanske inte har resurserna att vidta samma åtgärder som en större organisation. Detta betyder däremot inte att ett mindre företag skulle anstränga sig mindre för att uppnå en hög nivå av integritet. Vårt empiriska resultat pekar snarare på att det kan vara lättare för en mindre organisation att införa eller implementera integritetsåtgärder.

Dataminimering förekommer som en del av PbD:s ”Privacy as the Default” – princip och återfinns även i artikel 25 i Dataskyddsförordningen. I den forskning som vi har gått igenom framställs däremot inte dataminimering som en av de fundamentala delarna av ett integritetsarbete. Vårt empiriska resultat indikerar dock på att dataminimering kan vara en av de viktigaste grundpelarna för att säkra integritet i organisationer. En av organisationerna har anammat dataminimering till sitt yttersta och samlar således inte in några personuppgifter överhuvudtaget. Enligt organisationen i fråga leder detta till att de inte behöver behandla integritetsfrågor eller vidta åtgärder i samma utsträckning som andra bolag. Genom att inte samla in personuppgifter går det att argumentera för att organisationen uppnått en mycket hög nivå av integritetsskydd. Denna metod fungerar däremot inte i praktiken för alla organisationer. En av de andra organisationerna vi intervjuat kan exempelvis inte uppnå samma nivå av dataminimering eftersom myndigheter såsom Finansinspektionen, kräver att de samlar in och sparar persondata i viss utsträckning. Organisationens affärsmodell måste även behandla personuppgifter i viss mån för att de ska kunna erbjuda sina tjänster.

Att transformera PbD:s principer till implementerbara krav eller aktiviteter för systemutvecklare har i flera studier lyfts fram som en av de huvudsakliga utmaningarna med PbD. Organisationerna som vi intervjuat arbetar inte uttryckligen mot ansatsen PbD. Intervjupersonerna som vi talat med menar snarare att innehållet i principerna finns och ligger till grund för deras integritetsarbete. Något gediget arbete med att utforma denna typ av aktiviteter för hela ansatsen kan vi däremot inte se hos någon av de organisationer som vi intervjuat. Samtidigt ser vi inte heller att intervjupersonerna och deras organisationer lyfter denna problematik i någon större utsträckning under intervjuerna. Det tycks snarare vara så att organisationerna arbetar mot principerna omedvetet och tar fram egna lösningar där de anser att det behövs.

Samtliga organisationer som vi talat med är överens om att ett gediget integritetsarbete är ett sätt att bygga sitt varumärke. Trots detta återspeglas problematiken med att inte kunna se integritetsarbetets monetära värde hos två av organisationerna. En av organisationerna säger att de arbetar med integritet för att skapa tillit hos sina kunder och på så sätt genererar ytterligare affärsmöjligheter över tiden. Den andra organisationen säger att integritetsarbetet är strategiskt central och integritet är en viktig del av den produkt de erbjuder. Att värdera ett gediget integritetsarbete tycks vara svårt men samtliga organisationer är trots det överens om att integritetsarbetet i längden är gynnsamt.

På grund av PbD:s bredd är det egentligen väldigt svårt för organisationerna att inte möta ansatsen på några av dess principer. Även om alla organisationer exempelvis påvisade ett tydligt engagemang från ledningen eller att de nyttjade tekniska hjälpmedel såsom kryptering eller åtkomstkontroll, mötte ingen av organisationerna den övergripande filosofin med PbD. En av organisationerna visade däremot på en utgångspunkt till integritet som låg närmre Cavoukians värderingar. Att fullt ut efterleva de värderingar Cavoukian syftar till när hon säger ”Privacy must be embedded into every standard, protocol and process that touches our lives.” (Cavoukian, 2009, p.1-2), anser vi däremot vara en svår bedrift.

Appendix A

Tabell 7: Relaterad princip 1

Privacy as the Default	**GDPR**
Syftes specifikation	Artikel 5.1b
Insamlingsbegränsning	Artikel 5.1a Artikel 5.1c
Dataminimering	Artikel 5.1e
Begränsning av användning, lagring och avslöjande	Artikel 5.1e

Tabell 8: Relaterad princip 2

Visibility and Transparency	**GDPR**
Ansvarighet	Artikel 24 & 26
Öppenhet	Artikel 5.1a
Efterlevnad	Artikel 5.2, 12,13,14 (Tillsynsmyndighet och GDPR som rättsligt-bindande dokument)

Tabell 9: Relaterad princip 3

Respect for User Privacy	**GDPR**
Samtycke	Artikel 6.1a, 7, 8
Korrekthet	Artikel 5.1a & d
Tillgång	Artikel 12, 13, 14, 15, 16
Efterlevnad	Artikel 12,13,14 (Tillsynsmyndighet och GDPR som rättsligt-bindande dokument)

Appendix B

IS1 = Intervjusubjekt 1
Bank = IS1s arbetsgivare

#	**Person**	**Meningsinnehåll**	**Kod**
1	David	Perfekt. Sen också så har vi valt och det skrev vi också till dig i mailet att både du och företaget du jobbar för kommer att vara anonyma, vill bara dubbelkolla så att det är okej för dig, du vill inte att ditt namn ska synas eller?	
2	IS1	Inte om det inte är ett krav så behöver vi inte skylta med det vi kom fram till här helt enkelt. Kör på det!	
3	David	Vi kör det anonymt ja. Sen också, allt material som vi samlar in inklusive denna intervju, kommer bara användas till denna studie och det är bara jag Petter som har tillgång till den. Transkriberingen kommer ju synas men den kommer du också få tillgång till och möjlighet att korrigera och ge ditt OK på innan den färdigställs. Sen också så har du självklart rätt att avbryta intervjun eller direkt säga att där inte är någon fråga som du vill svara på så går vi vidare också så du är medveten om det. Då kör vi.	
4	IS1	Jag kanske ska säga några ord om mig också så ni vet vem jag är och faktiskt gör.	
5	Petter	Ja vi tänkte precis fråga dig här faktiskt, vi vill gärna höra lite bakgrund.	
6	IS1	Ja men jag jobbar som Principal architect på en avdelning som är vår IT-strategi, IT-strategi och arkitektur och jag är väl med och sätter de ramar som vi ska ha när vi utvecklar saker på banken. Bland annat policys, guidelines och vilka regler som vi måste följa för att vi ska klara av bland annat det ni pratar om så automatisk som möjligt. Det kanske inte ens behöver vara någonting som man ska behöva tänka på som utvecklar det bara finns där, By Design. Sådana frågor jobbar jag med, jag har varit här i fyra år på Banken och har jobbat på andra banker också. Jag är inte expert på det området som ni vill prata om men jag vet ju hur vi har löst saker och ting. Jag tror jag kommer kunna hjälpa er med svar på frågor helt enkelt. Kort sammanfattning.	ÖVT
7	Petter	Toppen, det låter ju som precis det vi söker i alla fall. Då har vi lite bakgrund där, och det är ju på Banken du sitter, vad är det egentligen Banken gör? Bara snabbt så man har det också.	

8	IS1	Banken riktar sig mot olika betallösningar. Så att om du har en webbhandel så kan vi erbjuda att de kan ta betalt via Swish, via kort, via, vilken betalningsmetod som helst. Men den stora grejen som vi tjäna pengar på är när man väljer att köra någon form av avbetalning. Låt oss säga att någon beställer på företag X för säg 10000kr och så får de en avbetalningsplan på 1000 kr i månaden i 10 månader så har de betalt av sin tv. Det är där vi tjänar pengar för vi tar ju då en avgift för det helt enkelt. Ibland kan det vara räntefritt men ibland så är det, vad ska man säga, andra prismodeller som gäller men det är upp till handlarna att bestämma helt enkelt. Sen har vi ju även vanliga kort, kreditkort, vi sysslar en del med business to business, med factoring, vi köper fakturor av folk som vill ha sina pengar snabbare. Säg att Nisses Bygg har gjort ett arbete och där är 3 månaders betalning på den men han behöver pengarna direkt, då kan han sälja fakturan till oss så tar vi en viss procent. Och sen så tar vi ju betalt då 3 månader senare av den som skulle betala pengarna till Nisses Bygg, fast dem pengarna går då till oss. Då blir det en kaka över helt enkelt. Vi sysslar också med vanlig utlåning om man behöver låna pengar. Inlåning har vi också. Det är nog våra huvudsakliga grejer som vi sysslar med.	ÖVT
9	Petter	Vi går in lite på hela Privacy by Design då. Du är säkert medveten om det men privacy är ju ett ganska vagt begrepp, det finns ju kanske inte någon direkt översättning till svenska men vi vill gärna veta hur du ser på begreppet Privacy?	
10	IS1	Jag tänker på det med integritet, skulle jag vilja säga. Information om våra kunder ska ju bara nås av dem som faktiskt har ett värde av att ta del av de, eller ska få lov att ta del av det. Det är inte så att vi ska slänga oss fritt med folks personnummer, adress och all den här ppi-datan, alltså det som identifierar en person. Det ska vara för de personer som har behovet, det är för dem det ska gälla. Det är "privacy" för mig. Du ska känna dig trygg när du kommer till Banken att den datan vi hanterar, vi hanterar väldigt mycket personuppgifter så klart, vi tar ju UC-rapporter och får all deras ekonomi och så vidare. Vi kan ta psd2 och vi kan fråga andra banker om hur det ser ut på dina konton hos andra banker och det kan vi ju göra för att kunden godkänner att vi gör det men det viktiga där är ju att vi ger en viss "trust" till kunden att vi använder det till det som vi är ute efter. I vårt fall kan det då vara en inkomstverifikation. När man ska söka pengar hos oss så får man ofta skriva in att "jag har den här månadslönen". Då kan vi ibland begära att du ska skicka in en löneslips så att vi kan lita på det. Ett sätt kan då vara att vi kontaktar andra banker och kollar, vad har de för inkomster helt enkelt, så kan det skötas helt automatisk. Den datan där, det gäller att vi hantera den så som vi har sagt att vi ska hantera den. För det är mig privacy.	BP, MM
11	Petter	Privacy by Design som approach eller ansats, du nämnde snabbt att ni arbetar efter konceptet i bakgrunden, men arbetar ni eft...	

12	IS1	Nämen jag skulle säga att vi tar det väldigt allvarligt. Vi har ju de här nödvändiga rollerna på banken. Vi har en DPO, data protection officer, vi har ju vår legal, vi har våra security. Det är ju av dem vi får de riktlinjer som vi behöver förhålla oss till vid utveckling, jag jobbar ju på utvecklingssidan. Vi har varit rätt så dåliga… Det kan jag lugnt erkänna. När jag började här för fyra år sedan så var det väldigt fritt. Alltså man kunde logga vad man ville och så vidare. Man tänkte mycket på affären, kör affären så att vi kan sälja så mycket som möjligt. Vissa grejer kom lite bakom. Då var vi inte så duktiga på privacy men det har vi faktiskt ändrat väldigt väldigt mycket på så nu varje gång vi utvecklar någonting och det är någonting nytt så har vi i princip ett protokoll som vi går igenom. Varenda tjänst som vi gör så klassificerar vi den och ser om den innehåller persondata eller inte och då hanteras de tjänsterna på ett annat sätt. Vi har fått mycket mer riktlinjer om vad vi får göra och inte får göra. Vi jobbar mycket nu med var vi loggar grejer. Vi måste ju logga vissa grejer, polisen kan ju ringa och säga, hur ser det ut på de här transaktionerna för den här tiden tillbaka och det kan vara en misstänkt brottsling till exempel. Så där kan man säga att vissa regler som kanske gäller för något bolag, där finns andra regler som står över de med det vi jobbar med och det måste vi ju hålla koll på. Vad kan vi deletea efter och en halv månad? När någon har skickat in en ansökan om ett lån som de inte tar, hur länge får vi lov att behålla den till exempel. Det kan finnas andra grejer som står över de regler som andra bolag, i och med att vi är en finansiell institution helt enkelt. Så det senaste fyra åren vill jag påstå att vi blivit väldigt, väldigt mycket bättre på det. Är vi perfekta? Nej det är vi ju inte, vi är ju människor och, ibland är vi kanske dåliga på att informera nya utvecklare om att “du kan inte logga personnummer här, du får inte, men så kommer det ändå ut där. Det har vi försökt stötta upp med att man måste använda sig utav vissa komponenter som vi använder när vi utvecklar, och dessa är lite “smarta” och upptäcker om det är känslig data och kan då maska den istället så att det sker per automatik. Det gör att utvecklare kan få lite mer laid-back approach till det, även om vi inte vill att de ska ha det, men där finns ett skyddsnät för att rädda upp vissa situationer. Är det komplett? Nej det är det inte. Men det är ändå någonting som vi jobbar med för att få det så säkert och stabilt som möjligt. Sen handlar det mycket om att man vill logga grejer, att man kan logga det på olika nivåer och på olika ställen. Ett ställe är där alla utvecklare ska få Access till grejer. Typisk situation som vi faktiskt får göra, det är att i felsökningsyfte, så måste vi kunna leta upp om	ÖVT, PED, UT, PR

		personen som har ringt in eller har problem med appen eller mina sidor, så ska vi hitta den personens, vad ska man säga, log eller session för att kunna hjälpa den personen. Där har vi ju ett ID och det är ju oftast personnummer. Det ska tilläggas då att det finns oftast bara på ett enda ställe, och sen så refererar till ett "ID" bara, som kan vara 1234567. Det är ju för att minska exponeringen. Därmed inte sagt att man inte kan koppla ihop det men det ska vara mycket svårare att göra det genom att bara ta en logg. Nu har vi ju lite utspritt så det är lite mer jobb för att kunna sätta ihop den datan. Alltså vi jobbar ju ständigt med detta att Privacy by Design som ni säger, att de ska bara finnas där.	
13	Petter	Men begreppet, det finns också där, ni använder er utav begreppet?	
14	IS1	Man kan säga så här, jag tror inte att alla känner till det och vi har haft den här approachen att mer utbilda, informera. Där använder vi inte direkt Privacy by Design men vi pratar i de termerna. Så kan jag säga. Om vi pratar med säkerhet och dem, Ja, då är det Privacy by Design. Visst språk fungerar inte på alla. Vi vill hålla det så enkelt som möjligt för våra utvecklare egentligen, och då är det "ni ska inte logga username, password", "ni ska inte logga kreditkortsnummer med expiry date" och så vidare. Vi pratar mer i dem termerna där. Du ska inte logga sådan data som gör att du kan knyta ihop någonting så att du kan ta över den personens roll. Det snackar vi rätt mycket om faktiskt. För loggar du ett username och password, tillsammans, kommer jag åt login så kan jag ju ta dem och logga in. Det är ju en big no, no! Så i dem termerna pratar vi mer.	UT
15	David	En snabb följdfråga där bara, när du säger att ni tänker på termer och så här, är det specifikt när ni pratar med utvecklarna eller rör det andra grupper också?	
16	IS1	Om man läser exempelvis GDPR, läser man de specifikationer eller de reglerna så är det ett visst sorts språk. Jag har ju försökt få till att vi översätter det språket till ett "Utvecklar-språk". Så vi har ju tagit en text som vi tycker fungerar för utvecklarna och egentligen vänt oss till vår "legal" och sagt "så här tänker vi förmedla det till våra utvecklare för att de kommer inte att läsa de här sidorna som de inte kommer att ta sig till". Vi behöver en översättning kan man säga, och då har vi fått godkänt på det. såsom "ja, prata så i de här termerna, det kommer att fungera, kör på det" så uppfyller vi ändå de kraven som vi har på oss helt enkelt.	ALH
17	Petter	Intressant, så det har ni alltså gjort tillsammans med era jurister då om jag förstår det rätt?	
18	IS1	Ja, vi tog och skrev utkastet och sen så har vi visat det och fått godkänt på att "ja men så här kan man också uttrycka sig" En lagtext är kanske inte för alla att läsa. Jag vill att man ska kunna uttrycka dem enklare men innebörden ska ändå vara densamma såklart.	UT

19	Petter	Ni arbetar ju helt klart med integritetsfrågor men varför arbetar ni egentligen med dem här frågorna?	
	IS1	Ja.… men det är ju än en gång, trovärdigheten. Vi måste vinna vår trovärdighet, alltså det är ju en sådan kamp om kunder, det är inte bara vi som sysslar med det som vi gör idag utan det är många ju. Kan vi då på ett trovärdigt sätt visa hur vi hanterar detta så är det ju guld. Sen så kommer det ju även anonyma kontroller ibland. Det kommer ju en eller två gånger om året. Då kommer juristfirman och verifierar att vi sköter oss och då måste vi kunna visa upp att vi sköter de här grejerna. Så visst, det hämmar ju vår utveckling för att vi lägger ju tid på saker som egentligen inte är en vinst för bolaget i form av pengar, alltså vi tjänar ju inga pengar för men i gengäld så vill ju vi vinna trust och det i sin tur kan ju ge pengar så det är en sidoeffekt av att vi är duktiga på detta. Vi vill ju hellre få ett betyg där det står AAA inom detta, det vill vi ju kunna stoltsera med istället för att, “shit de här kan ni inte göra affärer med, de avslöjar Allt inom hela Banken, man kan ju läsa allt om alla kunder” det är inte där vi vill landa. Sen är det ju så att vår styrelse faktiskt är personligt ansvariga och de vill ju, alltså det är ju tryckt därifrån att vi ska sköta oss. För det är inte utvecklarna i sig som råkar illa ut om vi gör någonting dumt, det är ju styrelsen. Det är deras ansvar. Får man den pressen att dem har den på sig, det är klart att dem vill att vi ska lösa detta. Därför tror jag att, det är väldigt stort fokus och det har kommit de senaste åren. Det var inte alls den fokusen för fem år sedan vill jag påstå.	MM, UT, PR
20	Petter	Så den här “Kulturen” som ni har kring integritet har liksom utvecklats på senare då?	
21	IS1	Ja det vill jag påstå, det har förändrats. Det har det. Jag kan inte säga exakt hur det är på affärssidan men på IT-sidan så är det ett helt annat tänk nu än för fem år sedan.	PR
22	David	När ungefär skedde den förändringen, uppskattningsvis?	
23	IS1	juni månad för fyra år sedan så hade jag min första presentation om detta. Så det var väl egentligen startskottet. Sen till att det blev implementation och att det faktiskt började exekvera någonting var kanske ett halvår senare, så låt säga att, 3.5 år vill jag påstå att vi haft full fokus på utvecklar sidan att tänka på de här bitarna.	
24	Petter	Kan man säga att ni har några metoder för att hantera dåliga integritetsbeslut och är det någonting som du i så fall satt med då på den tiden eller…	
25	IS1	Ja men det är också sånt som vi har dragit igång nu för typ 2,5 år sedan, och det är att vi har vårat IT-arkitekt-Forum. Vi har ju ett “strömlinjeformat sätt” att utveckla på och där har vi vissa regler. Följer man dem, jamen då är ens lösning i princip godkänd innan	PR, UT

		man kommer upp i det här arkitektur forumet. Men det är ju där vi granskar lösningar helt enkelt. Det är där som de som har gjort en lösning och vill sätta en lösning på plats i produktion får berätta om vad den innebär, en av frågorna där är "är det här känslig data eller inte?" Ja, är det inte det, då är det ju oftast grönt och köra vidare, men är det, då följer andra kontroller och då tittar vi väldigt noga på vad det är. Sen som jag sa innan, vi är ju bara människor. Vi har ju upptäckt att det har kommit upp grejer som borde tagit upp i ett sådant här arkitektur-forum där vi godkänner grejer som har struntat i att berätta det. Man har inte förstått allvaret, det har ju minskat väldigt mycket så det är sällan det händer nu. Senaste året så tror jag inte att det har hänt någon gång. Men i början så levde man kvar i det gamla vanliga att "Nej, vi gör lite som vi vill här, vilka regler ska vi förhålla oss till". Men det har blivit väldigt mycket bättre nu så nu är det som sagt, senaste året har det inte hänt någon gång att det har kommit upp någonting till produktion som är något som vi skulle skämmas för, om jag säger så.	
26	Petter	Så säkerställande, det har ni processer för, allting som kommer till produktion säkerställer ni? Där har ni givna processer för hur det sköts?	
27	IS1	Vi har givna processer och vi försöker att automatisera så mycket som möjligt av det. Den här manuella hanteringen det är ju vad det är. Ja, vi jobbar mycket med automation där. Att det ska bli säkert, direkt. då ska bli säker direkt Att man inte ska behöva tänka på det så mycket. Det är mycket det som vi kämpar med.	PR, MM
28	Petter	Upplever du att de här processerna då eller metoderna för att säkerställa att allting är på plats, upplever du att de förhindrar eller försvårar framtagandet av produkterna eller det flyter på?	
29	IS1	Det är både och. om man anammar de här reglerna och följa det, då går det väldigt fort att komma igenom vår process att få godkänt att komma till produktion. Men det finns ju alltid de som tycker sig veta bättre och då blir det jobbigare. Jag tycker vi har kommit rätt så långt även om vi har en liten bit kvar, men vi har kommit, vi har kommit långt. och det är på tapeten varje vecka att det här ska vi tänka på. Vi har ju obligatoriska utbildningar Jag har utbildningar, man måste gå en utbildning varje år som tar upp sådana här grejer och det är inte vi som har satt dem reglerna, det är ju finansinspektionen som säger att vi måste göra detta. Det gör alla. Från att man har en policy och process och så vidare så… Hur man får folk att följa det utan att agera polis, Det är ju det svåra. Det är jättesvårt vill jag påstå, det finns alltid en lucka om man vill hitta den, för att få ut grejer som inte är som de borde.	UT, FF, MM, PR

		Men vi har ju mer och mer monitorering på saker och ting. Det finns ju tjänster där som kan skanna igenom loggar på att hitta grejer och vi har ju alla möjliga sorters verktyg som vi är mer eller mindre bra på att nyttja, men... Vi lär oss hela tiden och blir bättre och bättre, även om jag tycker att vi är faktiskt är rätt bra just nu.	
30	Petter	Du pratar om utbildning, är det utbildning på alla nivåer så att säga eller har ni utbildning riktade till utvecklare i de här frågorna eller är det utbildning riktade till personer i din roll exempelvis?	
31	IS1	Det är en mycket bra fråga. Det är faktiskt en generell utbildning för hela Banken. Sen så finns det någonting som heter PCI-DSS som är om du hanterar kort. Det är för att man ska kunna hantera kortnummer, expire date och CVV koden, då måste man ha den certifieringen. Vi har outsource:at den delen, så det är ett annat bolag som håller dem grejerna så vi jobbar ju bara med referens-IDn. Vi har inga kortnummer och ingenting så vi behöver inte gå den utbildningen. Men om vi hade haft korten, då hade vi varit tvungna att ha en årlig utbildning som tar upp detta som är specifik för utvecklare. Men vi har inte den. Betyder det att jag är nöjd med det? Nej det är jag inte, jag skulle gärna vilja ha en utbildning ändå för att det här är så pass viktigt. Men, var sak tar sin tid och var strid har sin strid skulle jag vilja säga, men det här ligger på agendan att försöka ta upp. Så vi har ingen specifik kurs för utvecklarna, det har vi inte. Det vi däremot gör är att om vi har specifik kod som vi tycker är speciellt… "Det får inte finnas några luckor i detta", då har vi ofta en annan extern firma som är specialister inom säkerhet, då anlitar vi dem och så får de komma och granska koden och testa den och försöka knäcka den helt enkelt. Sen så får vi ett slutdokument av dem där dem antingen godkänner det eller så säger de vilka grejer som vi måste fixa för att de ska kunna godkänna det. Det har vi gjort på en del av våra komponenter som vi har. Just sådana komponenter är ju det som vi vill ska återanvändas av alla så att man inte utveckla en säkerhetsbov själv, utan man använda de komponenter som vi faktiskt har fått godkänt på utav en extern firma. På så sätt så jobbar vi med att bli "säkra" kan man väl säg.	PR, BP
32	Petter	Det låter som det ligger högst upp på priolistan det här, men upplever du att det prioriteras på samma sätt som designmodeler eller innovativa tekniker på den biten. Har det samma värde så att säga?	
33	IS1	Ja, men för vissa har det men jag skulle säga att affären kommer först. Om man skulle lägga en priolista så går affären först. Det ligger nästan över allt annat. Så om vi säger att vi måste onboarda den här e-handeln, det går före än att vi skulle hålla en utbildning för utvecklare i säkerhet. Med det sagt har vi ändå anställt en hel del personer som bara jobbar med säkerhet, som inte fanns på plats för fyra år sedan. Som har detta som sin främsta uppgift. Det var lite mer	FF, BP

		utspritt innan kan man väl säga, det är mer fokus nu men det är ändå inte högsta prion om du skulle jämföra med vilka affärer vi ska ta respektive om vi skulle titta på den här säkerhetsgrejen. Därmed inte sagt att vi tar lätt på det, det hoppas jag ni förstår utan vi tar fortfarande väldigt allvarligt på det.	
34	Petter	Detta hör ju lite till där men upplever du att detta sker genom hela produktens livscykel eller är det någonstans i produktens livscykel som det är större fokus?	
35	IS1	Bra fråga. Det är mest fokus när man sätter någonting nytt på plats. Då är det absolut mest fokus men sen kan det ske något under produktens livscykel. Det kan komma nya regler som vi måste implementera. Det är vi rätt så bra på att snappa upp. Då får vi ju modifiera i den produkten för att få det på plats. Men det är absolut störst fokus när det kommer på plats och sen så gäller det att ha koll på vad som händer. Där får vi ofta input från legal och security så det är inte så att utvecklare får ligga och leta efter vad som gäller, utan den informationen får vi till oss och sen får vi lägga upp en plan på hur vi anpassar oss och får in de grejerna. En sådan grej kan till exempel vara att innan kunde vi skicka ut mejl till vem som helst sen så kom det här med consent. Det är klart vi inte hade koll på att man var tvungen att få consent på grejer utan det var affären som kom och berättade att nu har de här reglerna kommit så nu måste vi fixa det. Så då tar vi tag och utvecklar eller köper ett system för det också får det komma in i processen att ta in den här consent datan och hur det funkar i de olika länderna och spara undan det så att varje gång vi ska skicka något reklamutskick så måste vi titta i vår consentdatabas. Ska Pelle ha mail eller ville han ha det på sms eller ville han inte ha det alls osv. Så saker och ting tillkommer hela tiden till våra tjänster och då får vi ta hand om det. Det är det som är jobbigt med legala krav, vi måste följa dem och när jag säger måste så måste man inte egentligen det. Du kan välja att ta risken. Det kan vara så att det kommer en regel så säger den att böterna är 10 miljoner. Då kan man ställa sig frågan, ska vi göra detta? Om vi skiter i att göra det så kommer vi tjäna 100 miljoner vilket betyder att om vi skulle bli påkomna då betalar vi 10 miljoner så har vi ändå tjänat 90 miljoner. Så det är en risk man tar och det är den riskmedvetenheten man ska ha hela tiden i allt vi ska efterfölja. Vi har valt att vi ska följa det som kommer, vi ska inte ta den här risken. Men ibland kan det vara att det ska vara implementerat om 6 månader, det finns inte ens chans i världen att vi hinner med det och då är vi rätt så öppna och meddelar och säger att vi börjat arbeta med detta men vi kommer inte klara av det, det kommer ta 9 månader för oss. Om man då pratar med myndigheterna så säger dem: aha, men då vet vi att ni jobbar med det och kommer få det på plats. Då kommer det inte vara någon risk att vi får böter under de tre månaderna. På det sätter vill jag nog säga att vi är öppna med vad vi jobbar med och har mot myndigheterna. Vi har en kanal där man kan anmäla risker anonymt och då kommer det in i vår riskdatabas. Vi har anmält grejer till finansinspektionen som har	EES

		kommit in där, och det är säkert vissa som säger: varför gör vi det? Det kunde vi hållit hemligt. Nä, det kommer bita en i svansen tillslut. Det är lika bra att vi är öppna. Till exempel om vi haft ett avbrott i 30 minuter, det innebar så och så för våra kunder. Så meddelar vi det. Sen om det blir böter eller om det blir en tillsägelse det är en annan femma, då får vi ta det för det som är grejen är att vi ska sköta oss och känna att det är bra att sköta sig, helt enkelt.	
36	Petter	Det är stort fokus på de legala kraven här. Det är ju så att flera av de principerna i Privacy by Design, anser vi, korrelerar väldigt väl med GDPR och de krav som ställts där. Vi utgår ifrån att folk som vi intervjuar följer GDPR och krav som öppenhet och samtycke osv. Men anser du att ni gör någonting utöver de legala kraven eller är det de som ligger till grund för hela Privacy by Design och integritets arbetet?	
37	IS1	Som sagt så tror jag vi gör ytterligare åtgärder. Just det här med att automatiskt kunna göra grejer, det är ingenting du behöver göra. Alltså det står ingenstans att du ska ha ett automatiskt flöde att maska bort kunddata. Det ska göras men vi göra allt för att det ska gå så smidigt som möjligt för oss, helt enkelt. Vi är väldigt nitiska i vår tolkning på grejer. Om vi tar inkomstverifiering som exempel, som är typisk GDPR där vi säger att vi vill samla in de här uppgifterna från andra banker för att ta reda på din inkomst. Då står det i vårt avtal ut mot kund, vad vi ska göra med den datan. Och då står där: vi ska ha den för att ta reda på din lön så att vi kan ge dig rätt förutsättningar för att få ett lån. Men det betyder inte att när vi frågar de andra bankerna att vi bara får den transaktionen som är lön, vi får alla transaktioner. Vi kan se om någon varit på Systembolaget tio gånger per vecka till exempel, så det är fullt möjligt. Men vi använder inte den datan. Vi kastar allt annat som inte har med just inkomstverifieringen att göra. Vi skulle ju haft jättemycket nytta av den andra datan för att kunna veta mycket mer om våra kunder. Men det är inte det de har svarat på att vi ska göra och därför kastar vi den. Och än en gång: hur kontrollerar man det? Det är jättesvårt, det handlar bara om trust, att det är vid säger det är det vi gör. Skulle vi då komma fram till att någon kommer att granska oss och hitta det här: alltså varför sparar ni alla kunders transaktioner på deras utgifter, ni skulle bara ta hand om deras inkomster. Då kommer det stå någonstans och det kommer bli en otrolig badwill. Hamnar du på förstasidan på Aftonbladet, den badwillen är så dyr så att vi tar inte den risken helt enkelt. Detta är tok viktigt vill jag påstå. Tycker jag att vi är helt för snäva i detta? Jo, men det tycker jag. Jag tror att om vi frågat och sagt lite mer vidta, vi vill samla ihop dina transaktioner för att vi kan hitta ett erbjudande till dig. Det kan ju vara så att vi får reda på att man betala på lån till tre andra långivare. Vi skulle kunna komma med ett erbjudande till dem som säger: samla ihop de tre och ta ett lån hos oss så får de här förutsättningarna. Vi skulle kunna vara proaktiva. Och faktiskt kunna ge ett bättre erbjudande till kunden. Men de har inte skrivit i avtalet mot kunden och därför kan vi inte	MM, FF

		göra det utan att skriva ett nytt avtal. Det är här jag skulle vilja ha det lite bredare. Det är inte så att vi vill vara onda mot kunderna, vi vill skapa affärer och det bygger på trust. Våra jurister är väldigt nitiska och vill hålla det väldigt snävt och det hämmar vår produktivitet i de vill göra med att bygga nya produkter och erbjuden.	
38	David	Du har nämnt lite utmaningar ni ställs inför och olika möjligheter med arbete, men känner du att där är något ytterligare du vill tillägga om ert integritetsarbete som till exempel är problematiskt eller skapar någon specifik möjlighet?	
39	IS1	Nja, jag tycker faktiskt vi jobbar bra och hela tiden bättre och bättre. Vi utmanar det som finns idag genom att försöka bli bättre. En sak om det här med loggarna, tidigare så hade alla tillgång till loggar och det är nu helt uppstyrt så du får tillgång till de loggarna som du ska ha tillgång till. Är du ansvarig för en tjänst då är det klart att du får gå in och titta i loggarna för den, men är du inte det då får du fråga den som är ansvarig som får ta fram uppgifterna åt dig om det anses lämpligt. Jag tycker nog att vi jobbar bra. Kan vi bli bättre? Vi kan alltid bli bättre i allt vi gör.	EES
40	Petter	Det samarbetet med jurister som du har pratat om, hur upplever du att det funkar? Är det ett samarbete som görs mellan jurister och ledning eller styrelse, eller är det med utvecklare också?	
41	IS1	Vi samarbetar men vi har helt olika synsätt på saker och ting. Vi lever i en värld där teknik tar över mer och mer och om vi ska ta en grej som vi brottas med nu så är det molnet. Vi har en analysavdelning som vill köra en analys på en massa data. De kan inte göra den som de vill för att vi har inte tillräckligt med processorkraft. Det skulle ta flera timmar att köra den. Skulle haft den datan i molnet så skulle vi haft oändligt med resurser och de skulle kunna köra sin analys på en timme och sen stängt ner de maskinerna och bara betalt för en timme. Här brottas vi just nu med att utbilda och lärare om vad det innebär att ha data i molnet som är väldigt på tapeten. Var får man lov att lägga där och vad får man inte lov att lägga där. Så samarbetet är där men som sagt vi har olika synsätt på risk och trust gällande den data som vi skulle vilja lägga ut i molnet för att kunna ta del av allt det som finns där. Om vi tar AWS till exempel som har så mycket tjänster som vi skulle kunna börja nyttja om vi fått ut data till molnet. Där finns andra bolag i Sverige till och med som kör allting i molnet och då utmanar vi lite: vad skiljer de sig från oss? Det är samma bransch, de har samma typ av persondata, det är samma typ av transaktioner, varför funkar det för dem? Det är det jag menar med att vi är väldigt snäva i vår tolkning vilket gör att vi hämmas av att kunna nyttja ny cool teknik som faktiskt skulle förbättra oss och göra oss ännu bättre. Om vi då tar AWS, det är klart de säger: lägg datan hos oss, det är inga problem. Jag tycker att det de säger kan de ju backa upp med väldigt bra data. Jag litar ju på att vi skulle kunna klara av vilken granskning som helst beroende på de lösningar vi väljer att få på plats när vi lägger	UT, FF

		data i molnet. Juristerna tolkar det lite annorlunda. Då gäller det att ha en dialog om var går er riskbenägenhet, när tycker ni det är okej att vi kan lägga ut grejer i molnet? Vi jobbar med detta just nu.	
42	Petter	Finns det några andra tillägg du skulle vela göra som kan vara relevanta för oss att kika på eller ha med i vår diskussion?	
43	IS1	Ja men det är det med kommunikation. Kommunikation med alla berörda parter, att försöka bilda förståelse. För att en avdelning har sitt synsätt och en annan har sitt synsätt, det beror på vilken roll du har i företaget. På något sätt gäller det att det samverkar för att alla de här avdelningarna, vi säger att det är en pusselbit, så är det rätt så tråkigt att bara sitta med en pusselbit, men när du har lagt hela pusslet och har en helikoptersyn och bara kan se att allting faller på plats, där kommer privacy by Design och det är kommer så mycket in då. Den pusselbiten blir så viktig att flera har förståelse för, så att man inte bara sitter med sina skygglappar på och bara tittar på sitt. Man måste kunna sprida blicken och se före nackdelar med saker och ting och ha den dialogen och då är det kommunikation, kommunikation, kommunikation. Sen om någon säger IS1: Du kan inte lägga detta i molnet, det förstår du väl? På grund av det och det och det. Också säger jag: Du förstår väl att vi måste lägga det i molnet, på grund av det och det och det. Då har man lite ett moment 22 och det är det man måste jobba med. Det är A och O. Jag vill påstå att vi jobbar med det varje dag för att kommunikationen.	
44	Petter	Du tog upp kommunikationen som en av de viktigare delarna med arbetet om jag förstod dig rätt? Att kommunikationen fungerar inom organisationen.	
45	IS1	Ja, men ta till exempel de som är på en C nivå, alltså CTO, CEO eller CFO. Ta en CTO, de behöver inte vara de mest supertekniska egentligen. Men de måste vara sjuk säljande. De måste sälja in den tekniken för andra som inte förstår sig på teknik. Hur gör man det? Det är bra kommunikation, kommunikation och att få den så enkel som möjligt. Ibland försöker jag träna på min fru: du jag skulle vilja göra detta, om jag skulle förklarar vad jag vill göra för dig, fattar du det då? På första försöket så förstod hon ingenting. När jag pratar med någon som inte förstår så tänker jag att jag ska prata med barn och förklara jag för dem. Sen kör jag några vändor med min fru också till slut så känner hon att hon förstår och då vet jag vilket språk jag ska använda när jag pratar med andra i hela bolaget. Man är en säljare på den nivån man sitter på för att få förståelse.	
46	David	Har du några andra frågor eller funderingar till oss, som du vill ställa?	
47		*Privat samtal fortsätter mellan intervjuledarna och IS1*	
48	IS1	Är det något ni behöver komplettera så hör av er	

49	Petter, David	Absolut.	
50	Petter	Vill du att vi ska skicka transkriberingen?	
51	IS1	Ska ni ändå skriva något så får ni gärna skicka det.	
52	David	Då skickar vi både transkriberingen och den färdiga uppsatsen så har du rubbet.	
53	IS1	Jättebra, tack så mycket.	
54	David	Stort tack för att du ställde upp.	
55	IS1	Stort lycka till.	
56	Petter, David	Tack så mycket, ha det gott!	
57	IS1, Petter, David	Hejdå.	

Appendix C

IS2 = Intervjusubjekt 2
Ad-tech-bolaget = IS2s arbetsgivare

#	**Person**	**Meningsinnehåll**	**Kod**
1	Petter	Lite bakgrund om dig och din roll på företaget som du sitter på idag, vad kommer du från för utbildning och så här, kan du dra en liten bakgrund?	
2	IS2	Absolut, så 2008 börjar väl egentligen min resa mot vad jag gör just nu. Började med att starta ett bolag som jobbar med textanalys. Det var precis i sin linda, det var precis när folk började prata machine-learning och AI på allvar. Vi jobbade med det under sju år innan de bolaget köptes upp av Ad-tech-bolaget, där jag jobbar. Jag var utvecklare under dem åren och under en tid var jag också hos Sony Mobile i Lund som Konsult under två år under eget kontrakt. När vi väl köptes upp så ville jag över till mer produkt fokuserat, inte bara jobba med utvecklingen som jag förvisso tyckte var superkul men jag var väldigt intresserad av beslutsprocesserna bakom vad vi byggde och så. 2015 gick jag över till en product-manager roll på Ad-tech-bolaget och 2019 ungefär så lämnade produktchefen på Ad-tech-bolaget, lämnade bolaget och i samband med det så tog jag över som produktchef. Sitter idag i vårt Management Team tillsammans med VD, finanschef, säljchef, marketeingchef. Utbildning, jag har ingen universitetsexamen, pluggat lite Maskinteknik, tyckte det var skittråkigt och hoppade av det, pluggat lite ekonomi efter ett halvår in där så kom den där punkten då, en kille ringde upp mig och sa att hen hade ett spännande bolag på gång och kollade om jag ville haka på det. Sen dess så har jag varit praktiserande snarare än studerande.	ÖVT
3	David	Vid den punkten där när du började på första bolaget, kunde du utveckla redan då? Var kom den kunskapen?	
4	IS2	Jag var en tämligen värdelös utvecklare skulle jag säga. Det var mer passion än talang. Jag hade ju börjat göra hemsidor, jag hade ett bolag innan det också som gjorde hemsidor till företag. Vilket egentligen var en katastrof, vi hade liksom ingen koll på någonting kring det här om "hur sparar vi data i databasen" fungerade det så var vi nöjda liksom. Men det hade varit väldigt lätt att komma åt den datan. Så 2008 då när vi kom över till första bolaget, eller började där så blev det ju allvar på ett helt annat sätt. Jag fick ju lära mig i takt med utmaningarna som vi stötte på vilket gjorde att motivationen att göra bra saker, läsa på, plugga var ju extremt hög för det var så mycket på och spel. Men jag är helt självlärd som	

		utvecklare och tycker väl själv att jag blev en duktig utvecklar med tiden och hade en arkitekt-roll på på Sony bland annat också. Men ibland kan man titta tillbaka på när folk pratar teori, "Vad fan menar dem nu liksom". Nej det är inte så mycket så, det mesta kan man lära sig själv också.	
5	David	Om vi går in mer på privacy här nu, hur skulle du beskriva begreppet privacy?	
6	IS2	För mig är det väldigt tätt förankrat till datan som andra har tillgängligt om dig, om dig som person då. Vad andra vet om dig, vad de samlar in om dig och i vilket syfte det sen används. Mot eller för din skull. Privacy är väl också för mig mycket, vilka val du gör och möjligheten att ha ett val överhuvudtaget kring hur du vill att din egna data ska behandlas, någon form av transparens kring hur information om dig brukas.	BP
7	David	Och anser du att ni på Ad-tech-bolaget arbetar enligt Privacy by Design som ansats?	
8	IS2	Till viss del, jag skulle säga att Ad-tech-bolaget har ett extremt stort fokus på privacy. Utgångspunkten i allt vi gör är: vilken data samlar vi in och I vilket syfte och behöver vi verkligen den datan och är svaret inte solklart ja på det så plockar vi inte ens in den datan som det ser ut. Vi har liksom inte aktivt sagt att vi jobbar med Privacy by Design men principerna vi följer, de kan du väl spåra tillbaka till Privacy by Design ganska väl skulle jag säga.	ALH, ÖVT
9	David	Varför tror du att ni jobbar med integritetsfrågor på Ad-tech-bolaget? Vad är motivationen? Vad är valet?	
10	IS2	Från början kommer det egentligen från att Ad-tech-bolaget jobba inom ad-tech industrin och jobbar med annonsering på nätet. Det är en industri som samlar in extremt mycket data om konsumenter i en skala som är helt sanslös. Finns uppenbara exempel som Google och Facebook men där vet väl alla i någon mån hur mycket data det faktiskt rör sig om, eller kan ha en känsla för det. Men det finns ju tusentals leverantörer som jobbar med annonsering som har tillgång till din data och i princip allt du gör online liksom. Ad-tech-bolaget, vi finns ju på stora publicisters sajter alltså nyhetssajter främst med vår annonsering. Jag vet då innan GDPR kom i effekt så kikade vi på hur många användare ser vi på daglig basis, jag tror det här var 2017 och då såg vi 30 miljoner unika användare över Europa. Och vi är ett litet bolag i sammanhanget. Datapunkterna som är tillgänglig kan vara allt från GPS koordinater till exakt vad har användaren läst och hur mycket de engagerat med olika typer av innehåll och så vidare. Det var och det är i stor grad fortfarande okänt för konsumenten, läsaren, att bolagen som sitter på all den här datan om dem att den överhuvudtaget finns. Så redan tidigt när Ad-tech-bolaget bildades så var väl, framförallt på utvecklarsidan, så var det folk som var ganska engagerade kring privacy frågor och hur din integritet eller personliga missbrukas i ad-tech-industrin. Det fanns liksom alltid	PR, MM, ALH

		kvar och det fanns alltid med när vi utvecklar saker med den här funderingen kring, "är det här okej att vi sitter på den här datan". Sen exploderade det här ju i och med GDPR för då för första gången så började ju bolagen på riktigt, man fick någonting att förhålla sig till, någonting som man skulle vara compliant med där industrin låg så otroligt långt ifrån de lagarna som helt plötsligt fanns på plats. I samband med det skiftet i slutet av 2017, 2018 då sa vi på Ad-tech-bolaget att vi ska släppa allt som har med personlig data att göra. Vi ska inte samla in personlig data om läsare längre. Vi ska jobba helt kontextuellt vilket ledde till konsekvensen att exempelvis cookies och IDn på användare, Cookies har ju använts i stor utsträckning för att följa vad en använder gör från site, till nästa site, till tredje site. De kunde vi helt plötsligt skippa, göra oss av med den biten. Det var mycket nya utmaningar och mycket nya liksom tekniska saker vi ställdes inför där vi behövde tänka annorlunda än industrin i stort. Samtidigt som vi strategiskt såg att det här är ett fält där vi kan göra någonting riktigt bra och där vi kan vara i framkant medan vi alltid kommer att vara, i bästa fall, en minimal spelare bredvid Google exempelvis, som sitter med data kring liksom exakt var har du rört dig, Vad har du sökt på, Vilka artiklar har du tittat på och så vidare. Vi var ju inte i stånd att konkurrera kring det. För vår del så fanns det då en strategisk vinning för bolaget så vi kan ju faktiskt differentiera oss genom att jobba fullständigt privacy safe och inte titta på unika användare.	
11	David	I den övergången till det mer kontextuella arbetet, innebär det då att ni inte har några personuppgifter alls då och inte egentligen behöver vara compliant med GDPR exempelvis?	
12	IS2	Precis, det blev ju liksom vår ingångspunkt i det hela. Vi tittade på GDPR och kollade på okej vi är här en leverantör som inte syns, du ser våra annonser, du ser våra artikelrekommendationer men de känns ju som en del av en nyhetssajt. Den enda indikatorn är att vår logotyp står under på vissa av de här placeringarna. Det finns liksom inga användare som har den typen av relation med oss. Och det är så pass komplext vad du gör med deras data. Att få ett informerat consent kändes extremt långt bort och det känns fortfarande extremt långt bort och det känns inte som att det låg i användarens intresse. Så därav så droppade vi helt personlig data	MM
13	David	Du kom in lite på det innan när du pratade om att när ni började, så fanns det redan personer som var insatta eller intresserade av privacy i någon mån. Hur skulle du beskriva att den företagskulturen ser ut idag i relation till privacy?	
14	IS2	Idag har det blivit en del av managementteamets stora fokus. Frånvaron av personlig data har ju blivit strategiskt central i hela organisationen, den påverkar allt vi gör idag så därför så är det ju det som vår marknadsavdelning skriver om, det är vad vår VD kommunicerar, det är vad jag som produktchef implementerar och för säljarna så är det som dem är ute och säljer in till annonsörer och	PR, MM

		publicister. Att här finns en trygghet, vi kan konkurrera med de som jobbar med personlig data fast du sitter inte med någon risk här att vi samlar in massa data som skulle kunna innebära att du får böter i framtiden.	
15	David	Eftersom ni jobbar så mycket med det, det är så pass tätt integrerat, har ni då några processer eller metoder också för att hantera den här typen av integritetsbeslut?	
16	IS2	När kommer till dokumentation och formella processer så är vi notoriskt dåliga skulle jag väl säga. Det kommer väl kanske lite av att vi fortfarande är ett bolag med väldigt starka start-up rötter. Det är alltid fokus på andra saker som man kan göra för att göra stor skillnad direkt och det är så pass lätt att sprida informationen i ett bolag som vårt där vi har som 50 anställda. Men det finns vissa grundprinciper och de börjar egentligen alltid ifrån vilken typ av data plockar vi in? Vilket är det helt centrala konceptet för oss. Har vi inte datan så är det så många bekymmer som försvinner längs vägen. Det är så många saker som vi normalt sätt skulle behöva kunna garantera eller ha koll på som vi inte ens behöver tänka på. Så den finns liksom inte överhuvudtaget i vår databas till exempel. Och det är väl också en sån sak som för tech-teamet, alltså om utgångspunkten alltid är, “det kan komma en dag då vår data läcker ut” hur mycket vi än jobbar med det, som ett litet team och även om vi skulle varit ett stort team som… Facebook hade ju en jätteläcka nu igen...så det är liksom en liten sak som du lägger in i din kod som kan läcka data eller som kan användas som en bakdörr in i vårt system för att komma åt data. Så med utgångspunkten att “samla bara in det vi kan stå för”, så gör det hela processen i alla fall väldigt mycket enklare.	PR, PED
17	David	Använder ni någon typ av riskbedömningsmetod eller liknande för att komma fram till det eller ni ser mer till dataminimering helt enkelt?	
18	IS2	Vi ser ju till dataminimering som vår främsta strategi. Sen när vi gjorde hela vårt GDPR-arbete då var vi ju genom hela systemet, alla punkterna där vi hade liksom någon typ av känslig data och kolla över “hur ska vi hantera det här för framtiden?” Tillsammans med kunder så är det ibland att du gör någon form av risk assessment där dem har sina frågor: “okej hur hanterar ni datan? Var sparas datan? Finns den i Europa? finns den utanför Europa? Är den krypterad? Är den encrypted in transit? Encrypted in rest? och så vidare. Så dem kommer väl upp regelbundet. Det jag tycker att vi saknar idag är liksom en strukturerad process för att internt löpande köra den typen av riskbedömningar. Där man exempelvis vart tredje månad går igenom och tittar och säger “ja men då tittar vi på de här punkterna igen, kolla vad som har förändrats och drar det över hela bolaget. Nu sitter jag mer på produkter och tech-sidan så mitt ansvar är ju främst “Vad har vi i våra databaser och vad samlar vi in? Men du har ju en sälj-sida också som jobbar med kunder. Läsarna som	ÖVT

		faktiskt ser våra artikel-rekommendationer är en sak men sen så har vi ju våra kunder, annonsörerna och publicisterna som har sina användare som är inne och jobbar med våra system och dem samlar vi liksom mer data omkring, hur de använder våra produkter exempelvis. Och våra säljare har liksom konversationer med dem på mejl och så vidare där det framkommer uppgifter som också är känslig privacy-mässigt. Dem sakerna kan jag säg att vi kan göra mer i framtiden för att ha strukturerade processer om liksom: Hur pratar personer, i en slack-konversationen eller hur sparar du datan i ditt CRM och så vidare. För att den faktiskt ska klara våra privacy antagen även på kundsidan.	
19	David	Tror du att det är någonting ni kommer att jobba fram eller det ligger någonstans mer i ett önsketänkande just nu? Eller det är faktiskt ett mål att ta fram de här processerna?	
20	IS2	Nämen det tror jag definitivt att vi kommer att göra och det är nästan ofrånkomligt idag, du måste liksom ha fokus på de. Jag tror att från vår del så är det väldigt mycket att ha någon form av privacy advocat, eller någon som är ansvarig för privacyfrågor på vår lönelista. Som faktiskt har det här som deras enda jobb att se till att alla delar av organisationen håller ihop och jobbar med personlig data på rätt sätt. Idag är det främst management teamet vid sidan av alla andra uppgifter som du har då som ansvarar för den processen och implementationen i organisationen. Då kan det lätt bli att vissa sådana frågor för lägre prioritet än de borde ha om du har en dedikerad person eller ett dedikerat team till privacy. Dit tror jag definitivt att vi kommer att komma.	
21	Petter	Du sa att ni kommunicerar med era kunder men är detta mer som en presentation för kunderna, alltså att ni alltid gör samma sak, eller varierar arbetet beroende på vad kunden vill också? Alltså att det skulle vara skräddarsydda lösningar?	
22	IS2	Det är en bra fråga. Ofta när de sker så är det så att du har en kund som själva har liksom ett långtgående privacy arbete och försöker säkerställa att deras leverantörer, dem de jobbar med, att de lever upp till deras krav, som kund. Så det kan vara så att de skickar över sitt riskbedömningsformulär och antingen så fyller vi bara i det och skicka tillbaka eller så kan det vara så att kunden har en intervju med oss för att förstå: hur hanterar ni lagring, vilken typ av data samlas in, i vilka olika syften samlas den in, hur används den i er säljavdelning osv.	MM
23	Petter	Men ni har liksom ett sätt att arbeta med det som de ofta är intresserad av då? Det är inte så att ni arbetar fram sätt att arbeta tillsammans?	
24	IS2	Nej precis, vårt svar blir alltid detsamma varje gång.	
25	David	Du som har lite koll på utveckling också upplever du att ert integritetsarbete på något sätt hindrar den tekniska framtagningen?	

26	IS2	Jag skulle säga nej, den gör att vi tänker annorlunda kring den tekniska utmaningen. När du går liksom tvärtemot industrin i stort och börjar tänka: hur ska vi göra det här, trots att vi inte har all data om individer som andra sitter på? Så ställs du inför helt nya tekniska utmaningar. Så någonstans så har det blivit så att vårt privacy-arbete de informerar våra tekniska utmaningar snarare än tvärtom. Vi innoverar och kommer med nya typer av lösningar i och med vårt privacy-arbete och summa summarum så ska jag säga att vi blir en snabbare organisation och snabbare tekniskt för det finns väldigt många frågor som vi inte behöver hantera när du inte ens samlar in data om en användare från början så är du väl lite som du behöver rensa ut till exempel. Du behöver inte ha så mycket processer kring att kontrollera att utrensningen har funkat som den, alltså: rensa upp i dina loggar, rensa upp i databaser, rensa upp i back-ups osv, för att du vet att ditt dataset innehåller inte personlig känslig information.	FF
27	David	Skulle du säga att detsamma gäller framtagandet av nya processer också, där ni måste ta hänsyn till integritet?	
28	IS2	Ja, vilken typ av processor tänker du på?	
29	David	Företags/organisatoriska processer	
30	IS2	Definitivt. När du har det här med läsarens eller konsumentens data och skyddet av deras data och inte överhuvudtaget inte samla in den. När du har det som grundstolpen i ditt företag så blir det att den automatiskt hänger med hela tiden. Det är alltid en fråga. När en konsument kommer in och säger: Vi vill att ni öppnar en youtube-video när det klickas på annonser, då blir direkt en fråga: vad händer med dataspridningen då? Vilka är involverade i att få del av datan och vem är det som tar ansvaret för det? Finns det några lösningar där det inte går att spåra användaren, finns det någon icke cookie-lösning eller liknande som man skulle kunna använda? Så ja, i princip alla processer i någon mån, så påverkar vår approach eller vårt tillvägagångssätt kring personligdata valen vi gör.	FF
31	David	Skulle du säga att ni prioritera privacy eller integritet på samma sätt som designmål eller tekniska lösningar?	
32	IS2	Absolut. Jag skulle till och med säga att privacy-målen är överordnade det tekniska. Vi kommer lite tillbaka till det här att privacy-målen informerar vilka tekniska innovationerna, snarare än att privacy begränsa vilka tekniska innovationer vi kan göra. Det är klart att det kommer vägval. Vi kan inte säga att om du har en annonsör som bara vill nå ut till kvinnor så kan vi inte plocka ut ett dataset, utan vi måste jobba på andra sätt för att uppnå liknande mål.	FF
33	David	Har ni någon typ av processer och/eller metoder för att säkerställa att integriteten inte försämras senare eller på andra steg i en tjänst eller produkts livscykel?	

34	IS2	Det är en bra fråga och när det kommer till de formella processerna som sagt, så är det inte vår starka sida. Men utgångspunkten är för oss alltid dataminimering av vad vi väljer att samla in. Så det är hela tiden den som vi måste ha koll på. När det kommer in en ny sak eller när jag som produktchef vill går i en viss riktning, vi ser ett visst problem där vi tror att det här kan vi lösa bättre än andra kan göra, vi kan hitta bra lösningar för våra kunder så tvingas du alltid att tänka på: Okej, vilken data kommer vi behöva för att kunna genomföra detta och faller det inom ramen för personlig data och att vi på något sätt behöver följa en användare i deras aktivitet på nätet, så går det bort. Då är det en sak som vi inte kan lösa det på det sättet, vi måste kika på andra sätt. På så vis finns den processen alltid med. Att fundera på vilken data vi samlar in. Vi har några uppgifter som är geografiskt område, det kan vara så att: finns användaren i Skåne eller finns de i norra Sverige och den datan baserar sig i grunden på ip-adress. IP-adress skulle jag kunna säga är känslig data, det skulle kunna säga någonting om en person. Så där behöver du då processerna för att se till: hur ser vi till att vi rensar upp datan, hur länge kan vi behålla datan, alla de åtagandena måste dokumenteras och finnas tillgänglig. Det står i våra privacy-policies som är öppet tillgänglig. Och hela snurra med hur vi hanterar back-ups osv. Där finns det en rutin. Återigen rutinerna är något som är liksom mycket mer knowledge, som finns inom teamet och kunskap om så här hanterar vi det, än formella processer, skulle jag säga.	EES, PED
35	David	Vem är det som bär ansvar för for privacy-frågor idag? Du sa att ni inte hade en uttalad person som jobbar med det men ni hade gärna velat ha det. Är ansvaret uppdelat eller hur ser det ut?	
36	IS2	Ja, där tycker jag att vi har en bit kvar att gå. Vi skulle vilja ha någon som har ett dedikerat ansvar för privacy som sen kan distribuera ut det i organisationen så att vi har någon form av utgångspunkt. Idag är det mycket mer så att det som gäller produktutveckling faller på mitt bord och det ansvarar jag för i egenskap som produktchef. Det är ett ansvar som jag skulle fått även om vi skulle haft någon som är ansvarig för privacy i det stora. Men då hade jag haft ett bollplank också. Någon som jag kunnat bolla med, kunnat kolla av med, kunnat diskutera och kunnat se att vi till exempel är inom gränserna här. På samma sätt så skulle kanske vår säljchef fått sina direktiv och haft sin dialog med en sådan mittpunkt, så att säga. Men idag så blir det mycket mer att i management-teamet där delas ansvaret upp och de olika managers som sedan tar det ner till kanske managers i nästa led. Så ansvarsfördelning absolut men definitivt något vi hade kunnat göra bättre.	
37	David	Hur ser det ut med någon typ av mekanismer får klagomål från konsumenter?	
38	IS2	Ja, det finns men där är kontakta oss via vår privacy email. Där finns en privacy policy med hänvisningar till hur du kan ta kontakt med oss och vi är ett fåtal människor som tar hand om de klagomålen.	

		Men sen i form av en strukturerad process så saknar vi en sådan. Och det är inte jättehögt på vår lista heller i och med att det som är konsument data, där har vi idag ingenting som är känsligt överhuvudtaget. Så om en konsument skulle komma till oss och säga att: Jag vill veta allt ni vet om mig. Så hade vi kunnat skicka tillbaka eposten som vi fick och säga att: Okej, nu vet vi din e-postadress och innan dess hade vi ingen aning om vem du var överhuvudtaget. Så det gör de lättare att hantera också.	
39	David	Är där några övriga utmaningar eller möjligheten du ser med ert integritets-arbete som du hade velat ta upp som du inte tidigare kommit in på?	
40	IS2	Industrin i stort har en enorm utmaning framför sig vad det gäller hur man ser på privacy och hur man hanterar användardata. För att ad-tech-industrin är enorm. Vad Google än lanserar så står deras annonsintäkter för ca 80 % av allt de tjänar. De är ett av världens största bolag och Facebook är samma sak och därtill så har du en hel drös av jättestora bolag som du aldrig hört namnet på som jobbar med massiva mängder data och som har investerat miljarder och åter miljarder för att bygga upp dataset om användare. Allt de användarna läser och koppla ihop det med finansiell data om de här användarna och sen så lägger du algoritmer ovanpå det för att för att förutspå: vad kommer intresserad den här användaren? Algoritmer som många inte har någon insyn i som kan få märkliga konsekvenser som att du radikaliserar människor genom att successivt visar mer och mer våldsamt innehåll exempelvis. Bara för att algoritmen på feedbacken att användaren spenderar mer och mer tid med oss. Så industrin har en jätteutmaning i hur beroende man är av den personliga datan och hur svårt det är att säga att: vi ska minimera hur mycket vi samlar in. För det får direkta konsekvenser för hur mycket pengar som de tjänar. I stället så har vi idag en tech-industri som är väldigt starka logister Washington till exempel och spenderar hur mycket pengar som helst för att påverka politiken eller politiker. Vilket för övrigt är en sak som om man tittar på vilka konsekvens får det att bolag sitter med så mycket information om så många användare. Har sett exempel på intresseorganisationer som riktar sin annonsering enbart mot kommunhus i Sverige exempelvis. Då kan du köpa användare och det är ganska få användare du måste köpa, och du kan köpa den för en rimlig peng men du kan alltid vara närvarande för dem när de är på Facebook, när de är ute på publicisters sajter, du kan få det att se ut som din fråga är det viktigaste som finns för väljarna. Medan de lever i en bubbla. Och det är bara för att de har identifierats som att de har en viss roll eller rör sig i ett visst geografiskt område, som i det här fallet. Så jag tycker det finns extremt stora utmaningar för industrin och för samhället i hur: vad ska vara tillåtet? Går du in och läser en nyhetstidning idag så är kanske inte din första tanke: Hur många 100 olika leverantörer får veta exakt vilken artikel jag läser och vilken typ av data kombinerar de ihop det med och var säljer de sedan den	

		datan vidare? Utifrån den utgångspunkten så gick ju ad-tech-bolaget till att hela problemet starta i att vi överhuvudtaget samla in den typen av information. Och vill vi göra en skillnad och lösa intressanta problem, då är det där vi ska börja. Så länge det finns kvar så kommer vi få bekymmer. Spekulerar man fritt så kan vi titta på USA och se hur demokrater och republikaner gått i två helt skilda riktningar och knappt kan prata med varandra. Det är så extremt olika platser och har skilda sanningar idag. Vad som är sant i det ena lägret är inte sant i det är andra. Det delar ett land mitt itu. Ser man på var har den resan börjat så tycker jag att det där var väldigt snabbt under de senaste tio-elva åren, under tiden som de sociala nätverken vuxit sig starka och de stora techbolagen har fått mer tillgång till användardata.	
41	David	Ja, det är klart en intressant diskussion. Där är mycket man kan säga om privacy.	
42	IS2	Ja, och där är en massa studier också på hur väl Facebook känner dig. Där man ser att efter 400 likes eller någonting sånt så visste de mer om dig än din partner och livskamrat. Det är helt sjukt, en nära kompis var väl 150 likes. Jag vet inte exakt siffrorna men det är helt sanslöst vad som går att göra med datan och hur mycket pengar det går att tjäna på att ha de och därav vilka starka intressen det finns för att inte användarna ska säga nej till att ge bort information om sig själva. Så det ser jag som en jätteutmaning för industrin. Dock ingen utmaning för oss. För oss är utmaningen mer: hur tjänar vi pengar när vi går en helt annan riktning? Hur fortsätter vi vara konkurrenskraftiga med någonting som är så annorlunda?	UT
43	David	Vad känner du Petter. Har du några tillägga?	
44	Petter	Nej jag tycker vi har fått ut mycket. Men det är väldigt intressant att ni lägger så mycket fokus på dataminimering även om det inte har samma fokus i privacy by design.	
45	IS2	Jo det är klart, när du lägger så mycket fokus på det området så får det en massa konsekvenser i så många led. Det minskar ju dina möjligheter i långt fler led och det gör också att du aldrig bygger upp ett dataset som du kan ta beslut på eller analysera i framtiden. Så det går helt emot gängse principer som funnits tidigare. Att samla in och spara så mycket data du bara kan, för du vet aldrig när du behöver den. Men det invaliderades helt av GDPR att du skulle kunna samla in data där du inte hade ett tydligt syfte.	
46	David	Har du några frågor eller funderingar IS2?	
47	IS2	Nej inte riktigt. Ifall det skulle vara något som ni kommer på där ni känner att ni skulle behövt förtydligande eller att förstår något kring vårt arbete så kan ni bara mejla mig.	
48	David	Absolut det gör vi i så fall. Jag skickar över transkriberingen så snart den är klara så kan du kika igenom den.	

49	IS2	Tack ska du.	
50	David	Tack för idag IS2. Stort tack för att du ville ställa upp.	
51	IS2	Inga problem. Hoppas det gav någonting.	
52	David	Jadå, det gjorde det gjorde det verkligen.	
53	Petter, David & IS2	Ha det gott, hejdå.	

Appendix D

IS3 = Intervjusubjekt 3
Konsultföretag = IS3s arbetsgivare

#	**Person**	**Meningsinnehåll**	**Kod**
1	Petter	Lite inledande frågor, vi är mycket nyfikna på hur du ser på begreppet privacy?	
2	IS3	Det beror ju på, I yrkessammanhang så handlar det om att säkerställa att användarna och de systemen jag implementerar oftast... Alltså såhär, Privacy är ju väldigt brett , i mitt privatliv handlar det om att säkerställa att mina uppgifter inte finns överallt och sådär, men om man ser det som yrkesroll så handlar det om att, oavsett vilka verksamheter jag är i så är jag antingen involverad i ett utvecklingsarbete eller så är jag med i ett ledningsarbete där jag rekryterar, jag jobbar med lönesättningar, jag jobba med personalsystem, jobbar mycket med CV-databas och såna grejer, och där är jag ju mer noggrann att kontrollera och säkerställa att vi får samla in de uppgifter som vi får och att säkerställa att det är "safe" liksom. Men det primära syftet eller primära liksom syn på privacy för mig är att säkerställa att vi har ett utvecklingsteam som har kompetens på det, så att vi har en kompetensspridning på det när vi bygger saker, hur vi lagrar data, var vi lagrar data, hur vi använder den datan, att det görs på ett framförallt lagligt sätt men också på ett etiskt sätt liksom. Det är väl så jag ser på det.	BP
3	Petter	Sen privacy by Design som ansats eller approach, är det något som du anser att du själv arbetar med eller ni på de olika företagen du arbetar med?	
4	IS3	Det beror på alltså jag är ju van vid att jobba i både stora organisationer och där är det väldigt strikt, där ska det ju genomsyra hela arbetet men jag tycker mycket av det arbetet har dykt upp, nu har jag aldrig använt begreppet Privacy by Design men det handlar mycket om att alla bolag har ju fått göra en självgranskning på grund av GDPR och allt det här men efter det så sker en helt annan approach, en helt annan oro mot det. Innan kunde det vara så här "amen personnummer" det är bara personuppgiftslagen som kommer att bry sig om det och det kommer ändå inte att hända någonting så man brydde sig inte riktigt som verksamhet men som utvecklare var man mer orolig. Men jag tycker absolut att det implementeras mer och nu måste vi tänka på det i varje steg av utvecklingen. Framför allt när vi har AD-användare och sådana saker. Hur använder vi den datan? Vart lagras den? Och framför allt att ha ett centralt AD så att vi inte behöver ha personuppgifter i alla system utan att ja, så att vi	ÖVT, MM, UT, EES

		bygger in det. Att vi har allting kapslat i ett område där vi faktiskt kan hämta den information vi behöver men vi använder det bara till den utsträckning som vi får.	
5	Petter	Men begreppet är ingenting som ni brukar?	
6	IS3	Nej jag skulle tro att om jag satt kvar på liksom STORKUND1 eller på STORKUND2 så kanske vi hade börjat använda det vid det här laget. Sen så är det också vilka system man sitter i. Sitter man i ett HR-relaterat system där det finns mycket personuppgifter då kanske man bygger mot det. Men sen när jag har suttit i stora verksamheter där det har varit väldigt lite personuppgifter, väldigt mycket produkter, alltså verktyg, den grejen då, det är användaren i sig som loggar in i systemet vars personuppgifter vi har hanterat men det har inte varit någonting där vi har behövt tänka så, vi har inte samlat känsliga data om människor eller ens knappt att vi har behövt en e-mailadress. Till skillnad från nu när jag sitter i ett system som vi ska bygga där vi både använder data hos dem anställda men där vi även kommer att behöva plocka personnummer från ett antal hundratusen om året i Sverige. Då blir det en helt annan situation.	
7	Petter	Och integritetsfrågor då, Varför arbetar ni med det egentligen?	
8	IS3	(glimten i ögat och ett skratt) Varför? för att våra kunder inte vill bli stämda och böta. Nej, Nej det är inte alls så utan generellt sätt så tycker jag att folk har vaknat till av hur data säljs och. det är i tiden och därför så får man säkerställa att man behandlar data på ett sätt som är etiskt och schysst mot ens användare precis som att man själv hade velat att bolag gör med ens egna data helt enkelt. Jag tror bara att det är mer och mer medvetet, det handlar inte lika mycket nu längre i dialogen om att “vi ska inte bli stämda, vi ska inte få böta” utan nu handlar det mer om att “Vad är rätt för användarna och vad behöver vi egentligen ha för data? “Det finns inget syfte att vi ska ha tre email adresser, hemadress plus målsmans samtliga uppgifter också, vi kanske kan nöja oss med det enklaste liksom”. Och sen säkerställa att vi kapslar in det på ett sätt och aldrig säljer den datan eller att den inte kan säljas, den inte går att få i en kontext där den kan säljas eller bli värdefull om den stjäls så att säga.	MM, EES
9	Petter	Skulle du påstå att ni har någon form av företagskulturer kring dessa frågor, kring integritet då?	
10	IS3	Alltså ja, jag skulle säga att mina kunder har det. Bolaget X som jag jobbar för är så pass litet att där handlar det mer om att… I med att vi inte bygger våra egna CV-hanteringssystem och såna saker, så när vi kvalitetssäkrar ett system som vi ska köpa in, då kollar vi på det, liksom “hur lagras den här datan, vad kan den användas till?” så tar vi det vidare sen. Men hos våra kunder så absolut, då finns kulturen att de ska skötas och att det finns någon som har centralt ansvarar för att, både vad vi lagrar för data, varför vi lagrar datan och sen även att säkerställa att den är trygg, dvs att man gör regelbundna pen-tester,	PR, BP

		man gör regelbundna liksom prover för att se "vad kan folk plocka ut och hur känslig data är det och Vilken typ av uppgifter är det dem kan hitta? Så kanske inte bara personuppgifter utan det är ju företagshemligheter också.	
11	Petter	Kan man säga då att ni har någon form av processer eller metoder för att hantera dåliga integritetsbeslut?	
12	IS3	Inga bestämda eller etablerade processer utan det är bara att det är mer eller mindre underförstått, i alla fall i dem teamen som jag jobbat med, att så fort det handlar om personuppgifter då tar man en extra fundering, framför allt när vi diskuterar arkitektur och design, alltså när vi diskuterar "Vad är det vi ska åstadkomma, vad behöver vi för uppgifter?" Då redan där i den processen så granskar vi "amen vilka personuppgifter behöver vi lagra och Vad ska vi göra med dem?" Så det finns ju absolut med i tänket, det är en del av att bygga ett system som har liksom, det är en del av kvalitetssäkringen nu för tiden, i alla fall i mina team. Att säkerställa att vi bygger kvalitativa saker och att det innefattar att vi hanterar integritet, att vi hanterar personuppgifter på rätt sätt, det är liksom som en "base-level" för oss. Jag har ju lyxen att, nästan uteslutande av mitt jobb innebär att jag kommer in på ett företag, jag bygger ett utvecklingsteam och sen så sätter vi liksom standarderna för det projektet. Det är ju inte alla som har det utan många kommer in i befintligt projekt, stora gamla drakar, så ska man hantera personuppgifter och integritet där liksom, det är svårare. Men i mitt fall så känns det ändå som en del av kvaliteten. Det avgör vilken arkitekt som jag väljer, Vilka utvecklare som jag väljer till mina projekt liksom.	PR, PED
13	Petter	Skulle du påstå att integriteten hindrar eller försvårar framtagandet av teknologier eller processer, eller produkter då i ert fall som ni utvecklar?	
14	IS3	Nä inte för oss. Det tycker jag inte, inte än i alla fall. Vi får se men jag tror att det till viss del förenklar för att det säkrar upp att vi måste ha standardiserade inloggningar, om vi ska använda personuppgifter på ett visst sätt då kanske vi måste ha någon form av BankID lösning, alltså den typen av inloggningar och det gör ju att det finns ju inte så mycket val utan vi får implementerar det här för att säkerställa att vi gör det säkraste möjliga valet för användarna och att dem är medvetna om, det finns liksom en annan medvetenhet om att dem faktiskt loggar in med sina personuppgifter, det tror jag är viktigt så att... Jag tror det är jobbigare för dem aktörerna som vill samla in data och sen sälja och där har jag aldrig varit.	FF, ÖVT
15	Petter	Ni brukar inte ha en person som är liksom ansvarig för de här frågorna i ert team eller det beror på vad är för produkt som ni ska bygga?	
16	IS3	Som de stora verksamheterna fungerar, då har de alltid ett Team eller en ansvarig och då får man egentligen deklarera vilken typ av uppgifter som vi vill spara och motivera det. Och då fanns det liksom	PR

		olika processer, Nu snackar vi STORKUND1, STORKUND2 den biten, då går de in och gör en analys på varför sparar vi det här, var lagrar vi den, utifrån det sätts det både säkerhetsklassning, det sätts andra regler på hur datan ska hanteras och så. I dagsläget där jag sitter i ett team med fyra utvecklare med en mindre organisation då är det någonting som ett, det finns alltid en GDPR ansvarig precis som det alltid finns ett skyddsombud eller något sådant. Dem är såklart involverade i vilka uppgifter som vi använder. och två, så väljer vi ju då utvecklar som har kompetenserna, som har utbildat och undervisat i det här som dessutom inte själv hade velat lägga in sina uppgifter i vad som helst. Som exempel så skulle vi köra gokart för två veckor sedan i teamet och i det här systemet så krävde dem att man skulle antingen logga in med Facebook för att registrera sig eller ta en bild. Hela teamet bara satte handflatan framför kameran och tog en bild, ingen av oss ville vara med i det systemet liksom. För att vi är så fixerade vid det här så att det är någonting som är med i vår process men sen är det klart att det är andra som skiter fullständigt i det liksom. Men jag tror att majoriteten har börjat fokusera mer på det. Det ni inte behöver uppleva så att säga är att komma in i, vi kom in i arbetslivet, jag började jobba 2013 tror jag, efter att jag hade tagit examen och då var det ju fritt blås, alltså man kunde göra vad fan man ville, man kunde samla hur mycket personuppgifter som helst. Det var inte lagligt men folk gjorde det ändå. Till den här skräcken som, alltså, jag skojar inte, oron och magkänslan hos många av de företag som jag jobbade för inför GDPR, det var en enorm grej. Nu i efterhand tycker man att det är lite löjligt så här men alltså jag vet inte hur många miljoner om inte upp mot miljarder vissa av de här bolagen har fått pumpa ner för att lösa dem här integritetsproblem. Nu kommer ju ni ut i en arbetsmarknad, om man väljer att börja jobba eller plugga vidare eller så men, där det ter sig ganska naturligt att ha det men skräcken som var där inför, när var det? 2018? Det är ganska komiskt att se tillbaka på. Det är verkligen ett skifte.	
17	Petter	Nu får du ju kolla ur kundernas perspektiv men prioriteras integritet på samma sätt som designmål och Innovation, alltså innovativa tekniska lösningar?	
18	IS3	Alltså, ja, njaa vi kan...eller det är väl snarare så här, vi får inte prioritera bort integriteten. Det är för stora konsekvenser ifall vi skulle göra det så att det står nästan högre än mycket annat.	FF
19	David	Om jag bara får flika in där, när ni ska göra den bedömningen mellan hur ni ska prioritera, hur väger ni i prioriteten då, vad mäter ni det mot? Är det legala dokument såsom typ GDPR eller ser ni även till de etiska aspekterna att nämen “vi måste prioritera det på grund av det också?”	
20	IS3	Jag har aldrig hamnat i en situation där jag behövt väga Innovation eller så mot integritet, så liksom, jag har aldrig varit i den situationen att jag behövt göra den. Det mesta finns workarounds på, till exempel att “ja men i stället för att vi lagrar de här grejerna i våra databaser så	

		kan vi lagra dem grejerna i AD:t och det AD:t får vi lagra det i. Är det så att vi landar i en situation där vi inte får göra det, då skulle vi sannolikt säga att amen, det finns egentligen ingen anledning för oss att lagra den typen av uppgifter. Och i annat fall får vi säkerställa att vi kan lösa det men, alltså vi bygger ju inga sociala, Vi bygger liksom inte något Instagram eller tik tok eller Snapchat där folk kommer att börja lägga in Jävligt konstiga saker och sen kan det knytas till deras person, alltså den typen av uppgifter hantera inte vi utan vi hanterar mycket affärsdata, det kan vara transaktionsdata det kan vara… Exempel jag började nu jobba för XX, jag vet inte om ni har körkort men om ni har tagit körkort de senaste åren så har ni säkert stött på något som heter XX?	
21	David	Hur länge har det funnits?	
22	IS3	Jag har faktiskt ingen aning men det vi gör är egentligen att vi håller på att bygga om hela det paketet liksom för att, det är egentligen där alla Sveriges körkortstagare ska in och utbilda sig. Och där kan vi ju stå inför en grej, amen okej, vi kommer att behöva personnummer för annars så kan vi inte verifiera att de faktiskt får vara med i systemet och får ta körkort. Vi kommer även behöva hantera ekonomiska transaktioner för att dem ska faktiskt boka sina körlektioner och dem ska registrera sina kurser och allt det här så vi kommer behöva hantera personuppgifter. Men då får vi ju helt enkelt säkerställa att dem personuppgifterna lagras på ett bra sätt och att vi anonymiserar datan i förhållandet av den. Att man inte kan knyta ihop transaktionsdata med personuppgifter hur enkelt som helst utan man får göra det lite svårt för eventuella “Hackers” eller vad man ska säg. Men att det godkänns på rätt sätt. Det är där jag menar att hade det varit så att folk ska ladda upp liksom bilder på sina hem och sina hundra och allting, då är det en annan sak men nu är det ganska strikt affärsmässig data som vi hanterar i de flesta system.	
23	Petter	Om vi kollar på hela produktens livscykel, kollar ni på integritetsfrågor genom hela produktens livscykel eller har mer fokus på någon av delarna?	
24	IS3	Jag hoppas det. Jag kommer in och så bygger jag nytt och sen så lämnar jag över till en förvaltning då och i den överlämningen till förvaltning så brukar ske någon form av eller så ska det ske en överlämning och de är införstådda med vad vi har för personuppgifter. Sen är det ju att data ska rensas med jämna mellanrum. Så det finns absolut en kontroll på det däremot så kan inte jag ta åt mig äran för att jag inte är med i den processen för då har jag ofta lämnat och är på nya uppdrag.	EES
25	Petter	Skulle du kunna ge något exempel på någon säkerhetsåtgärd ni gör vid överlämnandet eller någon gång?	

26	IS3	Det är väldigt beroende på vad det är för data men nu i de fall vi kommer behöva lagra persondata så kommer vi bara tillåtas att lagra det en specifik tid och den typen av arbete automatiserar vi i systemen så det inte blir beroende av personer. Det kommer bara informera en om att den processen kommer att ske, att den här datan om den ligger orörd så kommer de anonymiseras så att det inte går att knyta till en individ. Om inte den individen själv väljer att komma med sitt kundnummer. Men det ska inte finnas någon data som kan säga att det här kundnumret tillhör den här individen. Varken mailadress eller telefonnummer. Där får vi blåsa allting som inte är relevant för affären. Sen så har vi myndighetskrav på att kunna rapportera: hur många som genomför de här utbildningarna, de som lyckas, kvalitet på utbildningarna, de typen av saker så vi måste ha kvar viss typ av data men den kan anonymiseras så att det inte går att lokalisera vem det är eller var den här utbildningen skedde i landet.	EES
27	Petter	Kommunikationen mellan er och era kunder, vem är det du sitter och arbetar med?	
28	IS3	Ofta har de ett team som är blandat jurister och tekniker eller så har de någon som har blivit utbildad just för att hantera integritet, data privacy, och då har de ofta en övergripande roll för både persondata men även affärsdata och affärshemligheter. Det är betydligt känsligare på STORKUND1 än vad det är på STORKUND3 där jag sitter just för att STORKUND3 är bara trafikskolor, STORKUND1 sysslar med samhällskritisk infrastruktur så där var det känsligt av många anledningar. Till exempel kunde vi inte avslöja i våra system var vissa bevakningssystem fanns eller var vissa centraler fanns. Det fanns data där som vi inte fick eller visste om vad det var för att det blev så känsligt. Det var ingen i teamet, även om vi byggde för att hantera den typen av frågor, så fick vi aldrig veta var vissa saker fanns geografiskt för att risken och konsekvenserna om det kom ut var för stora.	
29	Petter	Men du upplevde att den är kommunikationen funkade fint mellan er liksom?	
30	IS3	I slutändan så är det kunden som är ansvarig för systemen. Jag levererar bara en tjänst som är per timme, men den kod som vi faktiskt skapar eller det material som vi levererar, det ägs i slutändan av kunden. Det är deras ansvar att vid drift att säkerställa att den är säker. Därför de ganska glada för att vi tar det ansvaret och att de får en helhetslösning.	MM
31	Petter	Kommer ni då med exempel på lösningar eller arbetar ni utefter deras policies?	
32	IS3	Det är ett samarbete. Om deras policy på något sätt skulle varit ett hinder och vi ser att det finns ingen legal anledning till att det skulle vara så, då kommer vi med feedback. Men det händer sällan. Det är snarare så att de har en policy som är lite lösare än vad vi är villiga att gå med på så vi gör det striktare i det systemet vi levererar än vad	UT

		de kanske har i sin övriga verksamhet. Så har det varit så här långt i alla fall, att man säger: men gör så här i stället, även om det kanske är legalt ok så kanske det är inte är vad vi anser är best practices. Då får vi säga till. Om de inte skulle vela ta det då blir det en större fråga: är vi villiga att leverera det här, men till någonting som vi anser är av sämre kvalitet? Ska vi då ta den diskussionen eller gör vi bara som kunden säger. tro det eller ej, men det är sällan vi bara gör som kunden säger.	
33	Petter	Finns några ytterligare utmaningar eller möjligheter med hela ert arbete som vi inte kommit in på tidigare?	
34	IS3	Nej, utmaningar tycker jag inte, utan det är mycket lättare än vad man förväntade sig än för fyra år sedan när man hörde om GDPR. Jag tycker generellt sett så känns det också betryggande att det man lämnar efter sig, när man har levererat en produkt, att det känns vettigt att användarna behandlas på rätt sätt och att man inte har ett spår efter sig av system som hanterar persondata på ett dåligt sätt. Jag kan tänka mig att de systemen som byggdes 2013, 2014 innan man visste om det här med GDPR. De systemen används många inte idag, men de som används skulle man gå in och göra en granskning på, om de inte har gjort det redan. Men allting som byggts efter med de här förutsättningarna, det behöver man fundera på det är bra eller det vet man att det är bra.	UT
35	David	Möjligheter med arbetet, du pratade lite om etiska aspekter innan, är det den primära motivatorn till att göra ett bra integritetsarbete?	
36	IS3	Förlåt vad sa du?	
37	David	Du pratade lite om etiska aspekter innan, att göra rätt för sig att man vill att företag ska behandla personuppgifter som man själv vill att de ska behandla ens egna. Är det din primära motivator för att göra ett bra integritetsarbete?	
38	IS3	Absolut, det är en kvalitetsstämpel. Att lämna någonting efter som inte gjorts snyggt det är inte kul. Dessutom så är det så att jag som produktägare har betydligt lättare att locka med mig mina konsulter som jag återanvänder i olika projekt. De flesta har jobbat med i två eller tre projekt tidigare så flyttar man med dem när man ska bygga något nytt någon annanstans. De följer bara med dig ifall de ser att jag tar bra beslut. Så för mig är det också en nyckel för att kunna leverera hos mina kunder och för att kunna bemanna projekten på ett schysst sätt. Utvecklarna som är väldigt måna om det här, mycket mer måna än management-folk, är intresserad av att jobba med mig vilket de blir av att göra det by the book. Inte bara när det gäller privacy men även arkitektur och ramverk och hur man ser på att vi inte gör några genvägar utan vi bygger på ett stabilt och långsiktigt sätt. Så det är bara en del av den övergripande kvalitetsstämpeln, både för mig i min yrkesroll så att jag kan gå till nästa kund och säga: vi byggde det så här och det används av de här kunderna och vi	MM

		gjorde det på det här sättet för att det skulle ha högsta möjliga kvalitet. Det är mycket lättare för mig att snacka in mig hos en kund som har den typen av behov senare. Det är ett varumärke också, framför allt när man frilansar så måste du ha ett bra varumärke med dig.	
39	David	Företagen ni utvecklar en produkt eller tjänst för, hur skulle du beskriva deras primära motivator? Är det framför allt att följa legala krav eller ser de andra möjligheter att realisera med integritetsarbete?	
40	IS3	Inte som jag stött på ännu, men det är inte omöjligt. Desto mer anonymiserad data de får lagra desto bättre. Jag kan tänka mig att historiskt sätt när man hade personuppgifter och affärsdata sammanknutet väldigt tajt, så gjorde det att det blev ett etiskt problem att göra stora big-dataanalyser. Nu tror jag dock många gjorde det ändå men nu i dagsläget när man separerar transaktioner, data för statistik och data som behövs för att kunna spåra mönster så till exempel min mor. Hon jobbar på STORKUND1 där de med hjälp av ny rensad och anonymiserad data kunde göra en analys på, med hjälp av lite machine-learning, gör en analys som visar på: Okej men hur beter sig en snitt kund i varuhuset? Vem tjänar vi mest på? Tjänar vi mest på den kunden som går igenom och kollar och köper en korv på vägen ut och sen beställa på nätet eller tjänar vi mest på den kunden som faktiskt är i varuhuset? Den typ av analys har man inte kunnat göra innan för att det var så mycket känslig data som till exempel var knutet till kontokort och man kunde inte sprida datan på samma sätt. Men nu är det bara affärsdata som är anonymiserad så det finns ingen spårbarhet men man kan fortfarande se olika mönster i beteende. Det visade sig att personen som köper en korv på vägen ut är den som STORKUND1 tjänar mest på. Det var ett exempel på att ju mindre känslig data du har desto mer kan du använda och sprida den i organisationen.	
41	David	Super. Har du något du vill tillägga Petter?	
42	Petter	Nej jag har fått vad jag är ute efter.	
43		* Privat samtal mellan intervjuledarna och IS3*	
44	IS3	Jag ska inte hålla er mer och lycka till med er uppsats.	
45	David	Stort tack för att du vill ställa upp. Vi skickar den färdiga uppsatsen när den är klar.	
46	IS3	Gör så. Ha det bra.	
47	Petter, David	Ha det gott.	

Referenser

Alshammari, M. & Simpson, A. (2017). Towards a Principled Approach for Engineering Privacy by Design, in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 10518 LNCS, 2017, pp.161–177, Available Online: http://link.springer.com/10.1007/978-3-319-67280-9_9. [Accessed 20 March 2021]

Bednar, K., Spiekermann, S. & Langheinrich, M. (2019). Engineering Privacy by Design: Are Engineers Ready to Live up to the Challenge?, *Information Society*, [e-journal] vol. 35, no. 3, pp.122–142, Available Online: https://doi.org/10.1080/01972243.2019.1583296. [Accessed 21 March 2021]

Bu, F., Wang, N., Jiang, B. & Liang, H. (2020). "Privacy by Design" Implementation: Information System Engineers' Perspective, *International Journal of Information Management*, [e-journal] vol. 53, no. April, p.102124, Available Online: https://doi.org/10.1016/j.ijinfomgt.2020.102124. [Accessed 19 March 2021]

Cavoukian, A. (2006). Creation of a Global Privacy Standard, [e-journal] pp.1–4, Available Online: http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf. [Accessed 20 March 2021]

Cavoukian, A. (2009). Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, *Information and Privacy Commissioner of Ontario, Canada*, [e-journal] p.5, Available Online: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf%5Cnwww.privacybydesign.ca. [Accessed 10 February 2021]

Cavoukian, A. (2010). Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D, *Identity in the Information Society*, [e-journal] vol. 3, no. 2, pp.247–251, Available Online: https://link.springer.com/content/pdf/10.1007/s12394-010-0062-y.pdf. [Accessed 18 March 2021]

Cavoukian, A. & Chibba, M. (2018). Start with Privacy by Design in All Big Data Applications, in S. Srinivasan (ed.), *Guide to Big Data Applications*, [e-book] Cham: Springer International Publishing, pp.29–48, Available Online: https://doi.org/10.1007/978-3-319-53817-4_2. [Accessed 18 March 2021]

Cavoukian, A., Taylor, S. & Abrams, M. E. (2010). Privacy by Design: Essential for Organizational Accountability and Strong Business Practices, *Identity in the Information Society*, vol. 3, no. 2, pp.405–413. [Accessed 16 March 2021]

Chen, S. & Williams, M.-A. (2013). Grounding Privacy-by-Design for Information Systems, in *Pacific Asia Conference on Information Systems*, 2013, p.15, Available Online: http://repository.usp.ac.fj/id/eprint/10038. [Accessed 20 March 2021]

EU. (2002). 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation), 2002 Europeiska Unionens Officiella Tidning 201, Available Online: https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=celex%3A32002L0058 [Accessed 19 March 2021]

EU. (2010). Europeiska Unionens Stadga Om de Grundläggande Rättigheterna, Available Online: https://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:sv:PDF. [Accessed 20 March 2021]
EU. (2012). Proposal for a Regulation of the European Parliament and of the Council COM (2012) 11 Final 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), Available Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011. [Accessed 10 March 2021]
EU. (2016). 2016/ 679 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), 2014 Europeiska Unionens Officiella Tidning 88, Available Online: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=SV. [Accessed 10 March 2021]
European Data Protection Supervisor. (2018). Preliminary Opinion on Privacy by Design, Available Online: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf. [Accessed 9 March 2021]
Gürses, S., Troncoso, C. & Diaz, C. (2011). Engineering Privacy by Design, *Computers, Privacy & Data Protection*, [e-journal] vol. 14, no. 3, p.25, Available Online: https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf. [Accessed 20 March 2021]
Gürses, S., Troncoso, C. & Diaz, C. (2015). Engineering Privacy by Design Reloaded, *Amsterdam Privacy Conference*, [e-journal] no. 610613, pp.1–21, Available Online: https://iapp.org/resources/article/engineering-privacy-by-design-reloaded/. [Accessed 20 March 2021]
Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S. & Balissa, A. (2018). Privacy by Designers: Software Developers' Privacy Mindset, *Empirical Software Engineering*, vol. 23, no. 1, pp.259–289. [Accessed 20 March 2021]
Hansen, M., Jensen, M. & Rost, M. (2015). Protection Goals for Privacy Engineering, *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, pp.159–166. [Accessed 20 March 2021]
Hustinx, P. (2010). Privacy by Design: Delivering the Promises, *Identity in the Information Society*, vol. 3, no. 2, pp.253–255. [Accessed 20 March 2021]
Insight Intelligence. (2021). Delade Meningar - Svenska Folkets Attityder till Digital Integritet 2021, [e-journal], Available Online: https://www.insightintelligence.se/wp-content/uploads/2021/02/deladeMeningar2021_Web_1-8A.pdf. [Accessed 20 March 2021]
Jacobsen, D. I. (2002). Vad, Hur Och Varför? Om Metodval i Företagsekonomi Och Andra Samhällsvetenskapliga Ämnen, edited by G. Sundin, Lund: Studentlitteratur AB.
Jacobsen, D. I. (2017). Hur genomför man undersökningar: introduktion till samhällsvetenskapliga metoder, edited by S. Andersson, Lund: Studentlitteratur AB.
Kroener, I. & Wright, D. (2014). A Strategy for Operationalizing Privacy by Design, *Information Society*, vol. 30, no. 5, pp.355–365. [Accessed 20 March 2021]
Ledarna.se. (n.d.) Ledarskap och chefens balansakt, Available Online: https://www.ledarna.se/utvecklas-som-chef/chefsrollen-och-ledarskapet/ledarskap-och-chefens-balansakt/ [Accessed 22 April 2021] [Accessed 20 March 2021]
Nationalencyklopedin.se. (n.d.) integritet, Available Online: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/integritet [Accessed 21 April 2021]
Oates, B. J. (2006). Researching Information Systems and Computing, *SAGE Publications*, Vol. 37.
OECD. (2013). The OECD Privacy Framework, *Organisation for Economic Co-Operation*

and Development, Available Online: [Accessed 20 March 2021]https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Schaar, P. (2010). Privacy by Design, *Identity in the Information Society*, vol. 3, no. 2, pp.267–274. [Accessed 20 March 2021]

Schultze, U. & Avital, M. (2011). Designing Interviews to Generate Rich Data for Information Systems Research, *Information and Organization*, [e-journal] vol. 21, no. 1, pp.1–16, Available Online: http://dx.doi.org/10.1016/j.infoandorg.2010.11.001. [Accessed 20 March 2021]

Senarath, A. & Arachchilage, N. A. G. (2018). Why Developers Cannot Embed Privacy into Software Systems?, *arXiv*. [Accessed 20 March 2021]

Spiekermann, S. (2012). The Challenges of Privacy by Design, *Communications of the ACM*, vol. 55, no. 7, pp.38–40. [Accessed 20 March 2021]

Spiekermann, S. & Cranor, L. F. (2009). Engineering Privacy, *IEEE Transactions on Software Engineering*, [e-journal] vol. 35, no. 1, pp.67–82, Available Online: http://ieeexplore.ieee.org/document/4657365/. [Accessed 20 March 2021]

van Lieshout, M., Kool, L., van Schoonhoven, B. & de Jonge, M. (2011). Privacy by Design: An Alternative to Existing Practice in Safeguarding Privacy, *Info*, vol. 13, no. 6, pp.55–68. [Accessed 20 March 2021]

van Rest, J., Boonstra, D., Everts, M., van Rijn, M. & van Paassen, R. (2014). Designing Privacy-by-Design, in B. Preneel & D. Ikonomou (eds), *Privacy Technologies and Policy*, Vol. 8319, [e-book] Berlin, Heidelberg: Springer Berlin Heidelberg, pp.55–72, Available Online: http://link.springer.com/10.1007/978-3-642-54069-1. [Accessed 20 March 2021]