Inbyggd integritet

Från koncept till praktiska åtgärder

Lukas Grönquist

Tobias Rydberg

Institutionen för data- och systemvetenskap

Examensarbete 15hp
Data- och systemvetenskap
Data- och systemvetenskap (180 hp)
Vårterminen 2017
Handledare: Esmiralda Moradian
Granskare: Patrik Hernwall
English title: Privacy by Design: From concept to practical measures

Stockholms universitet

Inbyggd integritet

Från koncept till praktiska åtgärder

Lukas Grönquist
Tobias Rydberg

Abstract

This study highlights the problem that arises when introducing the concept of privacy by design to organizations with already developed systems. The concept is based on seven principles, which together aim to create a strong privacy protection for the processed data. However, in previous research, the concept has been criticized for the fact that these principles are vague. The purpose of this study is therefore to clarify what can be done in organizations to comply with the principles of privacy by design. To answer the research question, how organizations with already developed systems can comply with the principles of privacy by design, a survey was made of current standards, measures, methods and processes, which then expounded into a document study. A selection of literature was made during several iterations to generate the most relevant literature for the study, which was then analyzed by conducting a content analysis. The result shows that there are measures to comply with each principle, but that the number of measures per principle varied. Thus, it may be more difficult to fulfill some principles than others. The study presents clear measures organizations can take to comply with the principles of privacy by design. Furthermore, the study clarifies what the principles and the concept of privacy by design means in practice.

Key Words:

privacy by design, information security, it-security, systems security, general data protection regulation.

Inbyggd integritet

Från koncept till praktiska åtgärder

Lukas Grönquist
Tobias Rydberg

Sammanfattning

Denna studie belyser problemet som uppstår vid införandet av konceptet inbyggd integritet i organisationer med redan utvecklade system. Konceptet grundar sig i sju principer, vilka tillsammans ämnar att skapa ett starkt integritetsskydd för den behandlade datan. Konceptet har i tidigare forskning dock fått kritik för att dess principer är vaga. Syftet med denna studie är således att klargöra vad som kan göras i organisationer för att uppfylla principerna för inbyggd integritet. För att besvara forskningsfrågan hur organisationer med redan utvecklade system kan uppfylla principerna för inbyggd integritet gjordes en kartläggning av nuvarande standarder, åtgärder, metoder och processer för att sedan utmynna i en dokumentstudie. Urval av litteratur gjordes under flera iterationer för att genom detta ta fram den mest relevanta litteraturen för studien, vilken sedan analyserades genom en innehållsanalys. Resultatet påvisar att det finns åtgärder för att uppfylla respektive princip, men att antalet åtgärder per princip varierade. Det kan därmed vara svårare att uppfylla vissa principer än andra. Studien presenterar konkreta åtgärder organisationer kan vidta för att uppfylla principerna för inbyggd integritet. Vidare tydliggör studien vad principerna och konceptet inbyggd integritet innebär i praktiken.

Nyckelord:

inbyggd integritet, informationssäkerhet, IT-säkerhet, systemsäkerhet, dataskyddsförordningen.

Synopsisformulär

BAKGRUND	De senaste årens digitalisering har lett till att personuppgifter och personlig information nu behandlas digitalt, detta har lett till att behandlingen sker i en allt större utsträckning än tidigare. Det har i och med detta utvecklats flera koncept och metoder för att skydda den personliga integriteten vid behandling i informationssystem, ett av de koncepten som har utvecklats är inbyggd integritet. Inbyggd integritet är ett koncept innehållandes sju principer vilka har blivit aktuella den senaste tiden, framförallt då den nya dataskyddsförordningen ställer krav på att organisationer implementerar inbyggd integritet i deras system. Arbetet hör till området för informationssäkerhet.
PROBLEM	Konceptet inbyggd integritet har existerat länge, trots det finns det en avsaknad av konkreta åtgärder som organisationer kan åta sig för att uppfylla konceptet. Att uppfylla konceptet utan att veta hur eller vad som kan göra är problemet som denna studie ska undersöka, med fokus på organisationer med redan utvecklade system.
FORSKNINGS FRÅGA	Forskningsfrågan för studien är följande “Hur kan organisationer med redan utvecklade system uppfylla principerna för inbyggd integritet?”. Forskningsfrågan är av intresse då konceptet för inbyggd integritet anses vara vagt, detta då det finns en avsaknad av konkreta åtgärder för att uppfylla konceptets principer.
METOD	För att besvara frågeställningen har en kartläggning genomförts, vilken har tillämpats genom en eftersökning av information om inbyggd integritet. Forskningsmetoden dokumentstudier har applicerats, där tre utvalda dokument har analyserats genom en innehållsanalys. För att ta fram säkerhetsåtgärder för att uppfylla principerna har dokument från ENISA, NIST och ISO analyserats.
RESULTAT	Resultatet av arbetet är ett antal skyddsåtgärder som organisationer kan implementera för att uppfylla respektive princip för inbyggd integritet. Åtgärderna och respektive princip som åtgärden uppfyller presenteras i en tabell. Genom detta resultat har arbetets frågeställning besvarats.
DISKUSSION	En begränsning i studien är valet av dokumentstudier som metod. Detta då det förutom åtgärderna som hittades i de utvalda dokumenten kan finnas ytterligare åtgärder i annan litteratur, som på grund av urvalet inte presenteras i studien. Slutsatsen från studien är att organisationer med redan utvecklade system kan uppfylla principerna för inbyggd integritet genom att implementera de presenterade åtgärderna. Detta är viktigt för samtliga organisationer i och med de kraven den nya dataskyddsförordningen ställer på organisationer. Arbetet leder inte till några etiska eller samhälleliga konsekvenser.

Innehållsförteckning

Figurförteckning

1 Inledning

I detta kapitel beskrivs bakgrunden till inbyggd integritet, vilket är det berörda ämnet i studien. I kapitlet presenteras även studiens bakgrund, problem, frågeställning, syfte och avgränsning.

1.1 Bakgrund

I takt med samhällets digitalisering lagras personuppgifter och personlig information digitalt i en allt större utsträckning, något som har lett till att insamling, lagring och behandling av detta görs i större skala och mer effektivt än tidigare (Solove, 2004). Det är dock inte bara en effektivisering av de medel som används vid behandlingen som har skett, utan antalet personuppgifter som behandlas har ökat i takt med att allt fler användare av internettjänster den senaste tiden har ökat (Siljee, 2015). Resultatet av detta är att den enskildes rätt att kontrollera vem som kan få tillgång till dennes privata information har försämrats (Danezis et al., 2014). Utöver att risken för att den enskildes rättigheter försämras innebär digitaliseringen även en risk för dataintrång, vilka även de har ökat de senaste åren (Hustinx, 2010). Vid flera av de större dataintrången som har ägt rum de senaste åren har personuppgifter blivit exponerade, stulna eller läckta (Gemalto, u.å).

Ovanstående anledningar kan ses som några av de faktorerna som ligger till grund för den nya dataskyddsförordningen som träder i kraft den 25 maj 2018. I Europaparlamentets och rådets förordning (2016/679) är kraven på individens rättigheter till personlig integritet större än någonsin, restriktionerna och skyddet vid behandling av personuppgifter är därför inte längre något organisationer som behandlar personuppgifter kan förbise. Förordningen berör såväl tekniska som organisatoriska åtgärder och kommer att gälla för samtliga medlemsländer inom Europa. Utöver en reglerad behandling för organisationer inom Europa kommer även tredjeländer som behandlar personuppgifter från europeiska medborgare behöva anpassa sig till förordningen. Detta då förordningen kräver att information om europeiska medborgare hanteras enligt den europeiska dataskyddslagen oavsett vilket land de behandlas i (ibid.).

I tidigare lagstadgar gällande behandling av personuppgifter har Europaparlamentet lämnat mer svängrum för nationella tolkningar i varje medlemsland vilket har lett till att olika länder har olika lagar gällande behandlingen av personuppgifter ser olika ut (ibid.).

Europaparlamentets kommande krav är dock hårdare, och samtliga medlemsländer och tredjeländer måste ta hänsyn till de nya kraven i Europaparlamentets och rådets förordning (2016/679). I de tidigare lagstadgar har inte överträdelser av lagen lett till sanktionsavgifter (Spiekermann, 2012), detta kommer däremot att ändras i och med Europaparlamentets och rådets förordning (2016/679).

Privacy by Design, vilket översätts till inbyggd integritet på svenska, är ett begrepp som under 90-talet togs fram för att ta itu med integritetsfrågor i samband med den ständigt växande informations- och kommunikationstekniken. Begreppet bygger på en samling principer vars huvudsakliga mål är att i ett tidigt skede ta hänsyn till de integritetsfrågor organisationer ställs inför vid hantering och utveckling av ett system (Datainspektionen, 2012). Utöver att applicera principerna i ett tidigt skede bör integritet även erbjudas som standard för användare (Koops & Leenes, 2013). I dataskyddsförordningen omnämns även konceptet under artikel 25 i Europaparlamentets och rådets förordning (2016/679).

Tanken med begreppet är att dessa principer ska stärka skyddet för den personliga integriteten i organisationers system samt affärsprocesser från början till slut, vilket går i linje med kraven i dataskyddsförordningen (ibid.). Principerna behandlar flera olika aspekter- från att arbeta proaktivt med säkerhetsåtgärder till att arbeta öppet och transparent mot användarna om hur deras uppgifter behandlas och vilka säkerhetsåtgärder som finns på plats för dem.
Organisationer som behandlar personlig information ska ta hänsyn till dessa principer under hela livscykeln för behandlingen - från insamling till radering (Cavoukian, 2011).
Sedan begreppet togs fram på 90-talet har det blivit ett vedertaget koncept för dataskydd, däremot är det en utmaning att ta konceptet till implementation (Kroener & Wright, 2014).

1.2 Problemformulering

Trots att inbyggd integritet de senaste åren har gått från att vara en rekommendation för att höja skyddet för personuppgifter till att bli ett regulativt krav finns det få konkreta åtgärder för att uppfylla konceptet och dess principer. Europaparlamentets och rådets förordning (2016/679) innehåller inte några konkreta riktlinjer på hur konceptet kan, eller bör implementeras- likaså kan riktlinjerna och ramverk utanför förordningen ses som bristande i detta avseende (Gürses et al., 2015). I tidigare forskning har just detta gap påpekats, gapet mellan konceptet och implementeringen av det (Kroener & Wright, 2014). Gapet gör att implementering av inbyggd integritet är något komplext. Dennedy et al. (2014) beskriver att inbyggd integritet snarare är ett ramverk för en tankegång än ett ramverk för implementering. Det har även gjorts få försök att översätta dessa principer till ett mer praktiskt ramverk (Stark et al., 2016).

Enligt Europaparlamentets och rådets förordning (2016/679) berör inbyggd integritet samtliga system som behandlar personuppgifter om europeiska medborgare. Detta skapar komplikationer när systemen i fråga redan är utvecklade, och inte tar hänsyn till principerna i inbyggd integritet. Kroener och Wright (2014) beskriver att personuppgifterna ska prägla hela systemutvecklingsprocessen, från initieringsfasen av projektet till avslutandefasen. Liknande komplikationer kan uppstå när nya system ska utvecklas - avsaknaden av konkreta åtgärder, riktlinjer och ramverk leder till att implementeringen av inbyggd integritet försvåras.

Problemet som ligger till grund för denna studie är således att det råder en avsaknad på konkreta åtgärder vid införandet av inbyggd integritet, samtidigt som Europaparlamentets och rådets förordning (2016/679) har stärkt kraven på skydd vid behandling av personuppgifter.

1.3 Frågeställning

Hur kan organisationer med redan utvecklade system uppfylla principerna för inbyggd integritet?

1.4 Syfte

Syftet med denna studie är att klargöra vad som kan göras för att uppfylla principerna för konceptet inbyggd integritet i organisationer med redan utvecklade system. Resultatet ska sedan kunna fungera som vägledning och implementeras i organisationer för att öka säkerheten och kontrollen över de personuppgifter som behandlas. Genom att presentera det teoretiska konceptet tillsammans med konkreta åtgärder konkretiseras konceptet till vad organisationer bör göra i praktiken. Detta är även något som har efterfrågats av Knowit Secure AB, med vilka studien i samråd är skriven med.

1.5 Avgränsning

I denna studie kommer antalet åtgärder att begränsas till högst 20 stycken för att kunna utföra studien inom den givna tidsramen. De standarder, åtgärder, processer och metoder som tas upp i denna studie kommer vara av generell natur för att på så sätt kunna vara applicerbara på största möjliga antal organisationer och system. Detta då dataskyddsförordningen berör samtliga system och organisationer som behandlar personuppgifter.

2 Vetenskaplig förankring

I detta kapitel beskrivs konceptet inbyggd integritet och dess principer, samt tidigare och relaterad forskning inom området informationssäkerhet. Slutligen beskrivs och sammanfattas de utvalda dokumenten studien bygger på.

2.1 Inbyggd integritet

Konceptet inbyggd integritet har funnits länge, och har utvecklats från Privacy Enhancing Technologies (integritetsstärkande tekniker). Själva uttrycket "Privacy by Design" myntades av Ann Cavoukian, där konceptet beskrivs utifrån sju stycken bärande principer (Cavoukian, 2011) vars syfte är att tillsammans stärka integritetsskyddet för personlig information som behandlas i organisationer. På senare år har konceptet blivit mer uppmärksammat bland annat i samband med den nya dataskyddsförordningen (Kroener & Wright, 2014).

Det finns utöver Ann Cavoukians principer andra riktlinjer för skydd av den personliga integriteten, däribland OECD:s principer för integritetsskydd (Organisation for Co-operation and Development [OECD], u.å). Några av de principer som OECD tar upp går att återfinna i Cavoukians (2011) principer för inbyggd integritet (Kroener & Wright, 2014). På grund av ovanstående anledningar kommer Cavoukians (2011) sju principerna för inbyggd integritet att användas.

I detta kapitel listas respektive princip (P*x*) för konceptet inbyggd integritet tillsammans med en beskrivning vad principen innebär. Principerna och dess beskrivning har sedan översatts till svenska. Den engelska benämningen för Cavoukians (2011) principer är:

P1. Proactive not Reactive; Preventative not Remedial
P2. Privacy as the Default Setting
P3. Privacy Embedded into Design
P4. Full Functionality - Positive-Sum, not Zero-Sum
P5. End-to-End Security - Full Lifecycle Protection
P6. Visibility and Transparency - Keep it Open
P7. Respect for User Privacy - Keep it User-Centric

De sju principerna tillsammans med respektive princips beskrivning (egen översättning):

P1. Proaktivt inte reaktivt; förebyggande inte botande

Att använda sig av medel för att proaktivt undvika att risker ska uppstå snarare än att vänta på att risker ska uppstå. Grundtanken bakom denna princip är att inte agera utefter vad för hot som realiseras, utan istället arbeta förebyggande mot dessa hot.

P2. Integritet som standard

Som standard ska maximal integritet användas för användare, en användare ska inte själv behöva välja vilka tillval i form säkerhetsåtgärder som används.

P3. Inbyggt skydd för personuppgifter

Dataskyddet ska vara inbyggt i designen och arkitekturen av IT-system och affärsprocesser. Dataskydd ska inte "läggas på" i efterhand. Resultatet av att arbeta efter denna princip är att integriteten blir en av grundfunktionerna i system och affärsprocesser - utan att påverka resterande funktioner.

P4. Full funktionalitet - inte ett nollsummespel

Användare ska inte behöva välja mellan integritet eller andra funktioner såsom exempelvis säkerhet. Det ska vara möjligt att erhålla både en hög grad integritet och säkerhet - inte antingen eller.

P5. Säkerhet från början till slut – skydd under hela livscykeln

Säkerhet ska appliceras i hela livscykeln av behandlingen av personuppgifter - från insamling till radering.

P6. Öppenhet och transparens

Intressenterna ska kunna säkerställa att oavsett vad för affärsprocesser eller tekniker som används vid behandlingen av personlig information ska säkerheten som utlovats efterföljas. Att arbeta med öppenhet och transparens mot användarna – gällande vad för uppgifter som behandlas och vad säkerheten vid behandlingen.

P7. Respekt för användaren

Användaren ligger i huvudfokus, respektera användaren genom att erbjuda användarvänliga inställningar.

Inbyggd integritet är ett ämne som figurerar i flera forskningsartiklar gällande den personliga integriteten i system. Tidigare forskning som enbart fokuserar på åtgärder för att uppfylla principerna för inbyggd integritet är dock begränsad (Kroener & Wright, 2014).

I tidigare forskning omnämns begreppet för inbyggd integritet som vagt, då konceptets principer lämnar många frågor om hur dessa faktiskt kan implementeras (Gürses et al., 2015). Forskning inom området har dock utförts, men har då varit av mer specifik karaktär. Gürses et al. (2015) har i deras studie ”Engineering Privacy by Design” undersökt hur integritetsskyddet för e-signaturer samt elektroniska tullar kan stärkas med hjälp av inbyggd integritet. Således har åtgärder för just dessa specifika områden diskuteras. Vad studien saknar är dock en koppling till de principer för inbyggd integritet Ann Cavoukian tar upp, då dessa inte listas i samband med lösningsförslagen. Utöver detta är resultatet av denna studie kopplad till två specifika områden. Detta gör att åtgärderna är svåra att generalisera och applicera inom andra organisationer och system.

I Rubenstein & Goods (2013) studie ”Privacy by Design: A counterfactual analysis of Google and Facebook privacy incidents” analyseras incidenter avseende personlig integritet hos företagen Google och Facebook, för att genom detta dra slutsatser om vad de hade kunnat göra för att undvika dessa. I studien diskuteras begreppet inbyggd integritet tillsammans med Cavoukians (2011) principer, men begreppet och dess principer knyts aldrig till de lösningsförslag som studien presenterar. Vidare är denna studie, likt den tidigare nämnda studien knuten till två specifika företag (Google och Facebook), vilket gör att resultatet blir svårare att generalisera och applicera hos andra organisationer och i andra typer av system.

Vad dessa studier gemensamt saknar är alltså en tydlig koppling mellan principerna för inbyggd integritet och vidtagna åtgärder. I och med detta förblir begreppet vagt, då principerna inte exemplifieras med hjälp av de vidtagna eller rekommenderade åtgärderna. För att klargöra hur organisationer med redan utvecklade system kan uppfylla principerna för inbyggd integritet kommer denna studie därför att vidare utforska åtgärder för konceptet, men även knyta dessa till principerna för inbyggd integritet.

2.2 Använd litteratur

För denna studie har ett antal dokument vars primära fokus ligger på skydd av den personliga integriteten valts ut som grund för studie. De utvalda artiklarna är "Privacy and Data Protection by Design" (European Union Agency for Network and Information Security [ENISA], 2014), "Security and Privacy Controls for Federal Information Systems and Organizations" (National Institute of Standards and Technology [NIST], 2013) och "ISO/IEC 29100: Information technology - Security techniques - Privacy framework" (International Organization for Standardization [ISO], 2011).

ENISA:s rapport (2014) fokuserar på olika tekniker som kan användas för att implementera integritetsskydd vid systemutveckling. Den syftar till att fylla gapet mellan legala krav och befintliga tekniska åtgärder. Rapporten innehåller både riktlinjer för design och andra mer administrativa kontroller som organisationer kan införa för att höja deras integritetsskydd. ENISA:s rapport ligger inom området inbyggd integritet, däremot utgår rapporten inte från Cavoukians (2011) principer för inbyggd integritet - vilket denna studie utgår från.

NIST:s (2013) dokument fokuserar på säkerhets- och integritetskontroller för informationssystem. Dokumentet består av flertalet säkerhet- och integritetskontroller som kan implementeras tillsammans med beskrivningar på vad dessa kontroller innebär. De åtgärder som NIST (2013) tar upp fungerar även att implementera och applicera i organisationer med redan utvecklade system, vilket krävs för att besvara forskningsfrågan. NIST fokuserar inte på begreppet inbyggd integritet, utan det fokuserar mer på framtagandet av konkreta åtgärder.

ISO (2011) är en internationell standard för att stärka den personliga integriteten i IT-system. Denna har valts då ISO-standarder är vedertagna inom branschen för IT- och informationssäkerhet. Den utvalda standarden ISO/IEC 29100 är framtagen för att förse organisationer med ett ramverk för ett starkt skydd mot personuppgifter inom informationssystem. Dokumentet är av generell natur och de framtagna åtgärderna kräver inga specifika förutsättningar för implementering (ISO, 2011).

Anledningar för val av ovannämnda dokument är att samtliga tar upp konkreta tekniker, kontroller och riktlinjer för att öka integritetsskyddet i informationssystem - vilket ligger till grund för att uppfylla studiens syfte. Däremot ställer ingen av de ovannämnda dokumenten upp deras presenterade åtgärder i relation till principerna för inbyggd integritet.

3 Metod

Studiens forskningsfråga besvaras genom en kartläggning. Kartläggningen har utförts genom en dokumentstudie där dokumenten har analyserats genom en innehållsanalys.

3.1 Forskningsstrategi

3.1.1 Vald forskningsstrategi: Kartläggning

För studien vars syfte är att undersöka vad som kan göras för att uppfylla principerna för konceptet inbyggd integritet har forskningsstrategin kartläggning valts.
Studien forskningsfråga kommer att kräva stora mängder data från ett flertal olika källor för att besvaras, vilket leder till att kartläggning är en lämplig strategi för studien. Informationen om skydd av personlig integritet och personuppgifter har eftersökts målmedvetet hos relevanta källor. Det målmedvetna eftersökandet av information är något som enligt Denscombe (2014) utmärker en kartläggning. Informationen som samlas in för att besvara frågeställningen kommer ha en väldigt bred täckning då den kommer att erhållas från ett flertal olika källor av olika natur. En av egenskaperna kartläggning har är att informationen som genereras har en väldigt bred täckning (Denscombe, 2014).

Denscombe (2014) beskriver att en avgörande faktor vid valet av forskningsstrategi är tillgången till data. För detta arbete är tillgången till data begränsad, detta då antalet tillgängliga respondenter som besitter tillräcklig kunskap inom inbyggd integritet anses vara för få för att använda som grund för studien. I och med detta reducerades de möjliga alternativ av forskningsstrategi till de som var möjliga att kombinera med dokumentstudier, vilken kartläggning är.

Av ovanstående anledningar har kartläggning valts som forskningsstrategi för studien.

3.1.2 Alternativ forskningsstrategi

En alternativ forskningsstrategi för denna studie hade kunnat vara fallstudier. En fördel med detta hade varit att den lämpar sig bättre när något ska undersökas mer detaljrikt (Denscombe, 2014).

I en fallstudie väljer forskaren ut en eller alternativt flera fall som grund för undersökningen, dock är det fördelaktigt att endast välja ett fall snarare än att angripa ett brett spektrum av fall (Denscombe, 2014). Då forskningsfrågan kräver en viss bredd och mest sannolikt ett flertal olika fall för att besvaras har denna forskningsstrategi valts bort.

3.2 Forskningsmetod

3.2.1 Vald forskningsmetod: Dokumentstudier

Som forskningsmetod använder sig denna studie av dokumentstudier, vilket som namnet tyder på är en typ av forskningsmetod där dokument används som grund vid informationsinsamlingen (Denscombe, 2014). Då det finns flertalet dokument inom området för informationssäkerhet lämpar sig denna metod bra för forskningsfrågan, då ett brett utbud av dokument innebär ett större och djupare område att utforska. Något som motiverar valet av dokumentstudier för denna studie är den begränsade tidsramen. Johannesson & Perjons (2014) beskriver att dokumentstudier är en forskningsmetod som lämpar sig väl när mycket data ska samlas in under en begränsad tid, vilket stärker valet av denna forskningsmetod.

För att utvärdera de insamlade källorna för studien kommer dessa att utvärderas enligt Denscombes (2014) kriterier för validitet. Kriterierna innefattar bland annat att utvärdera dokumentets pålitlighet, representativitet inom området, tydlighet och trovärdighet (ibid.). Utöver utvärderingen mot dessa kriterier kommer även majoriteten av källorna att vara granskade, vilket enligt Johannesson och Perjons (2014) tillför en högre tillförlitlighet till studien.

Denna studie är av kvalitativ natur där datan som används kommer att vara beskrivande snarare än mätande, vilket kännetecknar kvalitativ data (Johanneson & Perjons, 2014).

3.2.2 Alternativ forskningsmetod

Intervjuer är en forskningsmetod som hade kunnat användas för studien. Intervjuer är fördelaktig när datan som eftersträvas är i form av individers erfarenheter, något som för denna studie hade detta kunnat vara i form av individer som besitter kunskap och erfarenheter inom området för inbyggd integritet (Denscombe, 2014).

Denscombe (2014) beskriver att ett av de första stegen som forskare bör reflektera över innan valet av denna forskningsmetod är tillgången till potentiella respondenter.

Det har för denna studie beslutats att den givna tidsramen och forskarnas tillgång till respondenter som besitter kunskap och erfarenhet inom området för inbyggd integritet var för låg för att ha möjlighet att utföra denna forskningsmetod.

Utöver det begränsade antalet respondenter ska studien utföras inom en begränsad tidsram och intervjuer är en tidskrävande forskningsmetod (ibid.). Ett övervägande har gjort där det ansågs att nackdelarna vid användningen av denna metod vägde tyngre än fördelarna - därav har intervjuer inte använts.

3.3 Analysmetod

3.3.1 Vald analysmetod: Innehållsanalys

För att analysera dokumenten har analysmetoden innehållsanalys valts. Det finns flera olika tillvägagångssätt för att utföra en kvalitativ dataanalys, där en av dem är den innehållsanalys som kommer att användas i denna studie (Johannesson och Perjons, 2014). En innehållsanalys är ofta även induktiv, vilket betyder att forskaren försöker skapa en generell uppfattning under analysen snarare än specifik. För studien kommer flera dokument granskas utifrån deras innehåll, vilket sedan kommer analyseras för att skapa en generell uppfattning huruvida informationen i dokumenten förhåller sig till Cavoukians (2011) principer för inbyggd integritet.

Analysmetoden bygger på att en lämplig mängd text väljs ut för att analyseras, vilka sedan bryts ner till mindre enheter (Denscombe, 2014). Kategorier för dessa enheter tas sedan fram, exempelvis i form av nyckelord. Materialet kodifieras senare i förhållande till dessa, och när detta är gjort räknas frekvensen av hur ofta dessa enheter förekommer. När dessa steg är utförda kan en analys göras av texten utifrån hur ofta enheterna förekommer, samt relationen de har till andra förekommande enheter från texten (Denscombe, 2014). Denna analysmetod har valts på grund av forskningsfrågan, det som eftersöks för att besvara frågan kommer att bestå av flertalet åtgärder. För att kunna besvara forskningsfrågan i studien behövs medel för att kvantifiera innehållet i de utvalda dokumenten, vilket en innehållsanalys ger.

3.4 Forskningsetiska aspekter

Vid vetenskapliga undersökningar ska forskaren i fråga överväga huruvida undersökningen kan få negativa konsekvenser på de inblandade. Detta gäller i synnerhet för vetenskapliga undersökningar som berör individer, där konsekvenserna både kan vara kort- och långsiktiga (Vetenskapsrådet, 2011). Denna studie berör inte individer och leder således inte till att integriteten av några individer äventyras.

För denna studie har dokument använts som grund för informationsinsamlingen. Det är då viktigt att forskaren reflekterar och avgör källornas villkor för publicering (ibid.). Detta för att inte bryta mot den etiska aspekten att bryta mot källors villkor för publicering har de utvalda källorna granskats utifrån vad för villkor som gäller för parallellpublicering av dokumenten samt att upphovsrätten av källorna har granskats för att inte publicera sådant som är skyddat av upphovsrätten. Studien bryter således varken mot källornas villkor eller upphovsrätt.

Med tanke på valet av att utföra en dokumentstudie som bygger på dokument som andra har författat har forskarna refererat för att inte bryta etiken mot att plagiera andras arbeten (Vetenskapsrådet, 2011). Etiken är sällan ett problem när studien utgörs genom en dokumentstudie av publika dokument (Johannesson & Perjons, 2014).

För att avgöra forskningsetiken i detta arbete har studien utgått från Vetenskapsrådets (2011) rekommendationer för god forskningsed. Dessa rekommendationer har i studien efterföljts och är således en studie av god forskningsetik.

3.5 Metodtillämpning

3.5.1 Genomförande

För att samla in relevanta artiklar och källor för studien har Stockholms Universitetsbibliotek använts som primär databas. Sökorden har varit “privacy by design” tillsammans för filtret för “peer-review”. Utöver det har Google Scholar och ACM Digital Library använts med samma sökord som för Stockholms Universitetsbibliotek. Genom att granska de källor som återfunnits genom den valda metoden har även ytterligare källor undersökts. Det arbetet har gått till genom att gå vidare från referenserna i de utvalda källorna.

Utöver sökordet “privacy by design” har även “privacy engineering”, “privacy enhancing technologies”, “privacy”, “privacy implementation” använts som sökord i ovanstående databaser.

Utöver sökningar i dessa databaser har anställda på Knowit Secure AB tillfrågats efter trovärdiga och vedertagna källor som används inom branschen. Detta har fungerat som en vägledning i informationsinsamlingen och vidare möjliggjort tillgängligheten för branschstandarder.

För att ta fram relevanta dokument för studien gjordes inledningsvis ett första urval, vilket omfattade potentiell litteratur för studien. Kraven för att litteraturen skulle väljas var att de innehöll någon av söktermerna, samt att källorna var granskade för att stärka dess trovärdighet. För att stärka trovärdigheten ytterligare granskades dessa enligt Denscombes (2014) kriterier som omnämns i metodkapitlet i denna studie.

Det initiala urvalet genererade sammanlagd femton källor. Detta urval granskades sedan utifrån innehållet och ett andra urval gjordes baserat på de dokument som presenterade konkreta kontroller och riktlinjer för att höja skyddet av den personliga integriteten. Under det andra urvalet sållades många källor bort på grund av att de inte uppfyllde kraven som ställdes på källorna. Det andra urvalet ledde till att ENISA (2014), NIST (2013) och ISO (2011) valdes ut. Således började studien med ett stort urval av källor, för att sedan ebba ut till ett mindre, mer specifikt och relevant urval av litteratur. Både dokumentet från ENISA och NIST är publika dokument, etiken är då sällen ett problem (Johannesson & Perjons, 2014). Dokumentet från ISO är inte ett publikt dokument, men då den inte berör individer anses inte etiken av denna studie äventyras på grund av detta val.

Efter att källorna valts ut och utvärderats har en innehållsanalys gjorts enligt Denscombes (2014) riktlinjer. De åtgärder som presenteras i kolumnen under litteraturens namn i tabellen *(Tabell 1)* grundar sig på den rubrik som presenterats i samband med textstycket i litteraturen där den är funnen. Dessa har sedan sammanfattats och översatts till svenska termer för att användas i studien. Den sammanfattade översättningen presenteras i kolumnen åtgärd i tabellen.

Denscombe (2014) beskriver att forskaren vid en innehållsanalys ska ha en klar idé över vilka kategorier som ska användas, och vad som ska letas efter i texten för ändamålet av studien. Som beskrivet innan har Cavoukians (2011) principer för inbyggd integritet valts ut för studien och kommer därför att användas som kategorier för analysen.
Enheterna analyserades sedan utifrån deras frekvens samt dess relation till andra enheter funna i dokumenten. Efter att enheterna analyserats och beskrivits kategoriserades dessa efter de principerna som beskrivs för inbyggd integritet i den vetenskapliga förankringen. Principerna presenteras som överrubriker i resultatet medan de sammanställda åtgärderna presenteras som åtgärder under dess tillhörande kategori.

4 Resultat och analys

Resultatet av studien presenteras i tabellen nedan i form av i vilken litteratur åtgärden är funnen, samt litteraturens benämning på åtgärden. De åtgärder som har tagits fram under dokumentstudien har sedan aggregerats, vilket presenteras under kolumnen "Åtgärd".
En analys av åtgärderna har sedan gjorts för att kunna sätta dessa i relation till principerna för inbyggd integritet, vilka återfinns i tabellen under kolumnen "Kategori". Resultatet visar således vilka åtgärder som krävs för att uppfylla principerna för inbyggd integritet.

Åtgärderna presenteras sedan i en sammanställd text under dess tillhörande kategori.

Tabell 1: Sammanställning av åtgärder i relation till principerna för inbyggd integritet

Kategori	**Åtgärd**	**ISO**	**NIST**	**ENISA**
Proaktivt inte reaktivt; förebyggande inte botande	Medvetenhet och utbildning	Accountability	Privacy awareness and training	Promoting a deeper understanding
	Integritetspolicy	Privacy policies	Governance and privacy program	Enforce
Integritet som standard	Dataminimering	Collection limitation	Minimization of personally identifiable information	Minimise
	Ändamålsenlighet	Purpose legitimacy and specification	Purpose specification	Purpose binding
	Förstöring och återhållsamhet	Use, retention and disclosure limitation	Data retention and disposal	
Inbyggt skydd för personuppgifter	Konsekvensbedömning	Privacy compliance	Privacy impact and risk assessment	Privacy impact assessment
Full funktionalitet - inte ett nollsummespel	Behörighetskontroller	Privacy policy	Access Enforcement	Enforce
Säkerhet från början till slut - skydd under hela livscykeln	Pseudonymisering och anonymisering	Pseudonymous data	Minimization of personally identifiable information	Unlinkability

	Skydd vid lagring		Protection of information at rest	Storage privacy
Öppenhet och transparens	Transparens och öppenhet	Openness, transparency and notice	Privacy notice	Transparency
	Ansvar	Accountability	Complaint management	Accountability
Respekt för användaren	Datakvalitet	Accuracy and quality	Data quality	
	Tillgång för den registrerade	Individual participation and access	Individual access	Control

Tabellens kategorier listas nedan där varje princip (*Px*) för inbyggd integritet presenteras tillsammans med en sammanfattning av de tillhörande åtgärder som återfunnits i dokumentstudien *(Px.x)*.

P1 – Proaktivt inte reaktivt; förebyggande inte botande

P1.1 - Medvetenhet och utbildning

Målet med utbildningen ska vara att öka de anställdas förståelse inom ansvar och procedurer för den personliga integriteten. Den ska täcka utbildning inom hur de anställda kan identifiera risker, hur risker kan undvikas samt hur proceduren för incidenthantering ska gå till.

Dokumentera och implementera en uttömmande plan för att utbilda och öka medvetenheten hos de anställda inom organisationen.

Implementationen av utbildningen och kunskapsutbytet för att öka medvetenheten hos de anställda bör anpassas utefter de anställdas roller. Den bör även behandla:

a. Teoretisk utbildning.
b. Praktisk utbildning, exempelvis bör systemutvecklare utbildas enligt en praktisk metodik.

Arbetet bör ske iterativt och innehålla certifieringar för att uppmuntra lärdom samt bibehålla kunskapsnivån inom organisationen.

P1.2 - Integritetspolicy

Organisationen tar fram en eller flera policys som berör integritetsfrågor kring både system och affärsprocesser som behandlar personuppgifter.

En integritetspolicy bör inkludera ett åtagande att uppnå krav som är applicerbara på organisationen och berör integritetsskydd, samt åtagande att ständigt förbättra och utveckla detta integritetsskydd. Policyn bör även vara tillgänglig för samtliga intressenter, samt kommuniceras ut i organisationen.

Målet med detta är att säkerställa att systemet och affärsprocesser behandlar den personliga informationen på ett korrekt- och integritetssäkert sätt. För att uppfylla detta ska bästa praxis inom området för integritetsskydd granskas samt att roller för att upprätthålla policyn ska tilldelas. Policyn ska även kompletteras med tydlig dokumentation över metoder för att upprätthålla och efterleva policyn.

P2 - Integritet som standard

P2.1 - Dataminimering

Dataminimering handlar om att en organisation inte ska samla in mer personuppgifter än vad som krävs för ändamålet eller mer än vad som är tillåtet enligt lagstiftning. Utöver att begränsa mängden personuppgifter ska även naturen av personuppgifterna regleras beroende på ändamålet. För att minimera personuppgifter bör både insamlingen och bibehållandet av personuppgifter begränsas. Dessa riktlinjer och processer för att minimera personuppgifterna ska dokumenteras i policys för att upprätthålla minimeringen av personuppgifter.

Vid insamlingen av personuppgifter ska dataminimering erbjudas som standard vilket betyder att som standard samla in minimalt med personuppgifter – om möjligt inga alls. Detta kan lösas med hjälp av tekniker för anonymisering eller avidentifiering, vilka leder till en bibehållen integritet för den registrerade (individen behandlingen berör) samtidigt som organisationen kan använda sig av den insamlade informationen. (NIST har en guide för att anonymisera personuppgifter, publikationsnummer 800–122).

Utöver att minimera antalet personuppgifter bör organisationen även internt minimera exponeringen av personuppgifterna, vilket kan göras genom behörighetskontroller. En anställd ska enbart ha tillgång till personuppgifter som krävs för att utföra sitt arbete (Se P4.1).

P2.2 - Ändamålsenlighet

All insamling av personuppgifter som sker ska vara för att uppfylla ett ändamål, insamlingen ska vara explicit och vara förenlig med den information som utgavs vid registreringen. Informationen som ges ut till den registrerade ska vara skriven på ett tydligt språk för att undvika missförstånd. Ändamålet med insamlingen och behandling ska även ha stöd i lag.

För att undvika behandling som inte är ändamålsenlig bör ändamålen dokumenteras och de anställda som hanterar personuppgifterna ska genomgå en utbildning (se P1.2 - Medvetenhet och utbildning). Ytterligare en viktig åtgärd som går inom ramarna för ändamålsenlighet är att inte återanvända redan insamlad information för andra syften.

P2.3 - Förstöring och återhållsamhet

Behandlingen av personuppgifterna ska ske med återhållsamhet, endast sådan behandling som görs för att uppfylla syftet får göras. Efter att det förmedlade ändamålet är uppfyllt ska den insamlade informationen sluta behandlas samt förstöras eller anonymiseras. Anonymiseringen eller förstöringen ska ske på ett säkert sätt för att undvika att informationen försvinner, missbrukas eller blir tillgänglig för obehöriga. Detta gäller även för arkiverad eller kopierad information.

Om möjligt ska organisationen konfigurera informationssystemen så att datumen när informationen är insamlad, skapad samt när personuppgifterna ska förstöras eller arkiveras finns registrerade och uppdateras enligt schema. Detta för att förhindra personuppgifterna behandlas efter att ändamålet har uppfyllts.

P3 - Inbyggt skydd för personuppgifter

P3.1 - Konsekvensbedömning

Att utföra en konsekvensbedömning är grundläggande för att inom en organisation kunna behandla personuppgifter i ett system enligt principerna i inbyggd integritet. Det handlar om att dokumentera och implementera en process för konsekvensbedömning med avseende för att bedöma risken för individer vid insamling, lagring, överföring, användning och förstöring av personuppgifter. Det finns riktlinjer för hur och när en konsekvensbedömning ska utföras, NIST (2013) föreslår OMB Memorandum 03–22. ENISA (2013) föreslår i deras studie metoderna EBIOS och STRIDE.

En konsekvensbedömning ska ligga till grund för valet av säkerhetsåtgärder som implementeras, men även begränsa behandlingen av personuppgifter. Den lägger således även grunden för det fortsatta proaktiva och förebyggande arbetet.

P4 - Full funktionalitet - inte ett nollsummespel

P4.1 – Behörighetskontroller

Att införa behörighetskontroller är ett sätt att förstärka integritetsskyddet och informationssäkerheten i organisationen. Detta innebär att begränsa vad för information en användare har tillgång till i systemet samt vad denna användare får göra med informationen. Genom att begränsa mängden personuppgifter en användare har tillgång till reduceras exponeringen av informationen vilket är fördelaktigt utifrån ett informations- och integritetsperspektiv. Hur rättigheterna i systemen styrs ska dokumenteras i policys, vilket sedan ska implementeras i systemen (Se P1.2).

P5 - Säkerhet från början till slut – skydd under hela livscykeln

P5.1 - Pseudonymisering och anonymisering

För att minska möjligheten till att identifiera den registrerade, men samtidigt ha möjligheten att behandla personuppgifter kan pseudonymisering eller anonymisering göras. Vid pseudonymisering innebär detta att personen vars uppgifter behandlas istället behandlas under en pseudonym.

För att uppgifterna ska vara helt pseudonymiserade krävs det att de uppgifter som tillhör pseudonymen inte längre räcker till för att identifiera den ursprungliga personen. Detta då pseudonymiserad information går att härleda till en viss person om tillräckligt mycket data är länkad till samma pseudonym.

För att undvika detta kan istället anonymisering användas. Med detta avidentifieras all personlig information helt, vilket innebär att informationen inte längre går att knyta till en enskild individ.

P5.2 - Skydd vid lagring

För att personuppgifter ska vara skyddade under hela livscykeln och inte vara tillgängliga för några andra än behöriga användare krävs det att dessa även skyddas vid lagring. Med skydd vid lagring menas att datan inte är tillgänglig för obehöriga personer. Åtgärden syftar till att erhålla både integriteten och konfidentialiteten av de personuppgifter som lagras inom organisationen. Tekniker för att uppfylla detta är främst genom kryptering av data, brandväggar och system för att upptäcka intrång.

För att skydda data mot obehöriga är det även viktigt att en stark behörighetskontroll finns. Att flytta information till offline-baserad lagring kan även ses som en lösning för att skydda denna mot access via nätverk.

P6 – Öppenhet och transparens

P6.1 - Transparens och öppenhet

Transparens och öppenhet innebär att organisationen tydligt och på ett lättförståeligt sätt kommunicerar ut till intressenter hur de behandlar personuppgifter. Kommunikationen ska dels innehålla inom vilka lagrum behandlingen grundar sig på samt vilka medel som används vid behandlingen.

Denna information ska vara tillgängliga under samtliga faser av behandlingen, inkluderat både innan och efter behandlingen. Den ska även beröra vad som händer med informationen i dessa faser, vad som görs under själva behandlingen och vad organisationen gör när behandlingen är slutförd och ändamålet är uppfyllt.

Denna åtgärd inkluderar även att rapportera till de personer vars personuppgifter behandlas om något skulle ändras vid behandlingen eller om något skulle äventyra behandlingen.

Detta kan göras genom att offentliggöra organisationens policys som reglerar hur personuppgifterna behandlas och tillvägagångssätten för behandling av personuppgifter. Utöver detta är det även viktigt att möjlighet till dialog med personen vars personliga information behandlas finns. Sker ändringar av hur personuppgifterna behandlas är det viktigt att kunna kommunicera detta till samtliga berörda.

P6.2 - Ansvar

Att hantera personuppgifter medför ett ansvar att behandla dessa korrekt och förenligt med ändamålet med behandlingen som den registrerade har informerats om. Att förse den registrerade med information om hur behandlingen leder till ett högre förtroende för behandlingen hos den registrerade.
Några konkreta åtgärder som kan höja förtroende hos den registrerade att införa möjligheten för individen är:

a) Att införa möjligheten för individen att ställa frågor gällande behandlingen
b) Ge den registrerade möjligheten att klaga på behandlingen.

Förutom att öka förtroendet för organisationen hos den registrerade kan detta även fungera som extern insats för återkoppling vilket kan förbättra operationella modeller, användningen av teknik, datainsamlingsmetoder och även organisationens informations- och integritetsskydd. Funktionen för att klaga och ställa frågor ska vara enkel att använda och förse den registrerade med den informationen som krävs för att fullfölja handlingen.

Organisationens ansvar över personuppgifter innebär att både externa och interna kontroller över behandlingen tillåts, exempelvis externa eller interna revisioner.

P7 – Respekt för användaren

P7.1 - Datakvalitet

För att undvika att behandlingen av felaktiga personuppgifter sker, eller personuppgifter tillhörande en annan person än den registrerade individen behöver datakvalitén säkerställas. Genom att bekräfta att datan är korrekt, fullständig, relevant, uppdaterad och inte har kommer ändras över tid säkerställs datakvalitén.

Utöver att säkerställa datakvalitén vid insamling ska det även göras periodiska kontroller av personuppgifterna som behandlas, detta för att säkerställa att informationen inte är utdaterad.

Då organisationerna själva är ansvariga för att säkerställa datakvalitén behöver det införas kontroller och processer för att uppfylla detta.

En möjlig åtgärd för detta är att validera och korrigera adresser när de registreras, det finns automatiserade API:er (applikationsprogrammeringsgränssnitt**)** för adressverifiering. Ytterligare ett tillvägagångssätt för att förbättra datakvaliteten är att validera de insamlade personuppgifterna genom den registrerades förmyndare. Valideringen kan vid senare tillfällen ske kontinuerligt, antingen genom den registrerade eller genom dennes förmyndare.

P7.3 - Tillgång för den registrerade

Att ge den registrerade tillgång till sina personuppgifter som behandlas i systemen resulterar i att den registrerade får en ökad insikt i den personuppgiftsbehandling som berör dem och hur dessa uppgifter behandlas. Genom detta kan den registrerade säkerställa att informationen är korrekt, men även få möjligheten att besluta om en fortsatt behandling. Att tillåta tillgång för den registrerade kan även leda till förbättringar vid behandlingen då möjligheten till insyn kan leda till att information rättas och uppdateras.

Vid implementeringen av denna åtgärd är det viktigt att även införa rutiner och åtgärder för att säkerställa att den registrerade har rätt till informationen - att personen får ut sin information och inte någon annans.

5 Diskussion

Resultatet från studien visar på att det finns flertalet åtgärder som organisationer med redan utvecklade system kan använda sig av för att uppfylla principerna i konceptet inbyggd integritet. Därav besvaras studiens forskningsfråga ” Hur kan organisationer med redan utvecklade system uppfylla principerna för inbyggd integritet?”. Genom den utförda dokumentstudien har sammanlagt tretton stycken åtgärder identifierats, vilka sedan presenteras genom att sätta de i relation till definitionerna av principerna för inbyggd integritet.

Analysen med att sätta varje åtgärd i relation till principerna för inbyggd integritet utfördes genom att tyda den underliggande meningen med varje åtgärd - inbegripet målet med åtgärden. Målet med varje åtgärd sattes sedan i relation till de olika principernas krav för att se om målet av åtgärden fyllde principens krav. Vissa principer hade tydligare krav medan andra var mer abstrakta, och det slutgiltiga resultatet togs fram efter flera iterationer av analyser.

Något som tidigare har påpekats i studien är komplikationerna som uppstår när en organisation ska implementera inbyggd integritet i deras redan utvecklade system. Att ta principerna från teori till implementering är en utmaning då det saknas en praktisk tillämpning av inbyggd integritet (Kroener & Wright, 2014). Studiens resultat är således eftersökt i tidigare forskning. Det tidigare teoretiska konceptet har genom studien konkretiserats då resultatet består av en praktisk vägledning i form av åtgärder inom konceptets principer.

Bidraget med studien är att de identifierade åtgärderna konkretiserar konceptet och ger riktlinjer på hur principerna för inbyggd integritet kan uppfyllas, något som i tidigare forskning har varit vag (Gürses et al., 2015). Tidigare forskning inom området för inbyggd integritet har även i flera rapporter varit bristande med avseende på deras generella riktlinjer och åtgärder, både Gürses et al. (2015) och Rubenstein & Goods (2013) studier har mer organisations- och systemspecifika åtgärder. Denna studies presenterade åtgärder avser att vara av generell natur för att på så sätt vara applicerbara på största möjliga antal system och organisationer. Studiens bidrag är även något som har efterfrågats av Knowit Secure AB.

Det är således detta som leder till resultatets signifikans och originalitet.

Studiens resultat visar på att det utifrån litteraturen finns ett oenhetligt antal åtgärder för respektive princip, vilket kan tyda på att några av principerna för inbyggd integritet är svårare att uppfylla än andra. Utifrån studien kunde exempelvis bara en åtgärd kopplas till principerna "Full funktionalitet - inte ett nollsummespel" och "Inbyggd skydd för personuppgifter". En bidragande faktor till detta kan vara att åtgärderna som eftersöktes under studien var av generell natur, när det för dessa principer kan krävas mer verksamhetsanpassade åtgärder för att uppfylla principerna.

Något som ytterligare motiverar viktigheten av studiens resultat är Europaparlamentets och rådets förordning (2016/679) som kräver att organisationer bygger in skyddet av personlig information i deras system. Flera av de framtagna åtgärderna går att återfinna som krav i förordningen bland annat uppgiftsminimering och ändamålsenlighet (ibid.). Att studiens resultat kan hjälpa organisationer i deras arbete med att efterleva dataskyddsförordningen leder till att företag kan undgå de sanktionsavgifter som är en påföljd av att inte följa förordningen (ibid.). Det är tidigare nämnt att studiens resultat är av mer generell natur än tidigare forskning, vilket leder till att ännu fler organisationer kan ta stöd och använda de framtagna åtgärderna.

Studien var avgränsad till att ta fram så generella åtgärder som möjligt, för att genom detta resultera i en applicerbarhet för största möjliga antal organisationer och system. Trots denna avgränsning finns det dock en risk för att vissa organisationer och system av mer specifik karaktär inte har möjlighet att implementera de presenterade åtgärderna. System som dessa åtgärder är generaliserbara för kan således variera beroende på hur pass flexibla dessa är. Ett system som redan regleras av andra lagar där strikta affärsprocesser måste efterlevas, eller har utvecklats för så pass länge sedan att det inte längre är möjligt att göra stora ändringar i, kan därför ha svårt att tillämpa generella åtgärder. Resultatet från denna studie är däremot mer sannolik att vara tillämpbar på fler system än tidigare omnämnd forskning i detta avsnitt, vilken har varit riktad till mer specifika system. Detta då denna studie med hjälp av dess avgränsning strävat efter en bred tillämpbarhet till skillnad från tidigare utförda studier.

5.1 Begränsningar

En begränsning i denna studie är datainsamlingsmetoden, i dokumentstudier blir forskarna begränsade till det som går att finna i dokumenten som används i studien. Det kan således utöver de åtgärder som presenteras i studiens resultat finnas ytterligare åtgärder som inte identifierades från de utvalda dokumenten. Denna begränsning skulle även kunna vara en av faktorerna som ledde till oenigheten av principernas åtgärder som beskrivs i studiens diskussion.

Något som återspeglas i flera av källorna som har studerats är att mätningar inom inbyggd integritet saknas. Studien har kunnat visa på hur en organisation kan uppfylla principerna för inbyggd integritet, men inte i vilken grad detta kan göras. I och med detta var det svårt att i studien avgöra hur pass väl en princip faktiskt uppfylldes genom dess tillhörande åtgärd, detta är något som kan ses som ytterligare en begränsning i studien.

5.2 Trovärdighet

I en kvalitativ studie som denna arbetar forskaren nära datan, både i insamlings- och analysfasen, vilket kan leda till att andra forskare har svårt att reproducera ett identiskt resultat (Denscombe, 2014).

Genom att använda information från flera olika källor och av olika karaktär stärks trovärdigheten i studien. Som grund i dokumentstudien har dokument från NIST (2013), ENISA (2014) och ISO (2011) använts, vilka som beskrivet i den vetenskapliga förankringen är av olika karaktär.

För att avgöra validiteten i dokument som ligger till grund för studien har Denscombes (2014) kriterier för validitet använts. Dessa kriterier är dokumentets äkthet, representativitet, mening, syfte och trovärdighet. Då samtliga aktörer som stått bakom de utvalda dokumenten är etablerade och vedertagna inom branschen för informationssäkerhet kan trovärdigheten ses som hög för dessa. De utvalda dokumenten är även representativa för dessa aktörer då dokumenten är inom området för informationssäkerhet. Dokumenten syftar till att hjälpa organisationer att höja deras säkerhets- och integritetsskydd och är hämtade från respektive aktörs hemsida. Då denna studie bygger på dessa validerade dokument kan även denna studies validitet ses som hög. Vidare har även dokumenten analyserats noggrant vilket stärker studiens trovärdighet ytterligare (ibid.).

Likt validiteten kan även reliabiliteten i en kvalitativ studie anses vara svår att avgöra. När datan som används i studien är kvalitativ finns det risk för att olika forskare med hjälp av samma data får fram olika resultat (ibid.). Åtgärderna som presenteras i studiens resultat är inhämtade från NIST (2013), ENISA (2014) och ISO (2011) där källorna flera gånger omnämnde samma åtgärder vilket stärker trovärdigheten för de presenterade åtgärderna.

5.3 Etiska och samhälleliga konsekvenser

Denna studie leder inte till några etiska eller samhälleliga konsekvenser. Studien är utförd i enlighet med Vetenskapsrådets (2011) forskningsetiska principer. Datan som använts i studien innehåller säkerhetsåtgärder från dokument och är inte insamlad från undersökningsdeltagare. Datan i studien berör således inte några individer och äventyrar därigenom inte integriteten hos några individer. Inte heller studiens resultat leder till några etiska eller samhälleliga konsekvenser.

5.4 Framtida forskning

Något som påpekats under studiens diskussion är att det inte går att mäta inbyggd integritet, detta är således ett område för framtida forskning - hur inbyggd integritet kan mätas. Det uppmärksammades under denna studie att det är svårt att avgöra hur väl en åtgärd uppfyller principerna för inbyggd integritet. Att i framtida forskning undersöka konceptet och dess principer på ett ytterligare djup och därigenom ta fram ett ramverk för att mäta inbyggd integritet kommer inte bara vara nödvändigt för ytterligare framtida forskning - utan även för organisationer vid implementeringen av inbyggd integritet.

5.5 Slutsats

Frågeställningen i studien “Hur kan organisationer med redan utvecklade system uppfylla principerna för inbyggd integritet?” har i studien besvarats. Utifrån studiens resultat går det att dra slutsatsen att det finns flertalet åtgärder organisationer med redan utvecklade system kan implementera för att uppfylla de olika principerna för inbyggd integritet. Samtliga principer för konceptet har i studien konkretiserats genom minst en åtgärd för respektive princip. Syftet för studien var att klargöra vad organisationer med redan utvecklade system kan göra för att uppfylla principerna för konceptet. Således är även syftet för studien uppfyllts, organisationer kan använda resultatet som en vägledning vid implementeringen av inbyggd integritet.

Något som har omnämnts tidigare i studien är att inbyggd integritet är svårt att förstå då det råder en avsaknad av konkreta åtgärder för att uppfylla konceptet. Därför är ytterligare en slutsats som kan dras att konceptet tydliggörs genom de åtgärder som presenteras.

Referenser

Cavoukian, Ann, 2011. *Privacy by Design The 7 foundational principles.* https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (Hämtad 2017-02-22)

European Union Agency for Network and Information Security (ENISA). 2014. *Privacy and Data Protection by Design-from policy to engineering*. doi: 10.2824/38623.

Datainspektionen. 2012. *Inbyggd integritet*. Datainspektionen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/ (Hämtad 2017-02-20).

Dennedy, Michelle F., Fox, Jonathan och Finneran, Thomas R. 2014. *The privacy engineer's manifesto: Getting from policy to code to QA to value*. New York: Apress Open. E-bok.

Denscombe, Martyn. 2014. *The good research guide: for small-scale social research projects*. 5. uppl. Berkshire: McGraw-Hill Education. E-bok.

Europaparlamentets och rådets förordning 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Gemalto. [u.å]. *Breach level index.* Gemalto. http://breachlevelindex.com/top-data-breaches (Hämtad 2017-02-21).

Gürses, Seda, Carmela Troncoso, and Claudia Diaz. 2015. *Engineering privacy by design reloaded*. I Amsterdam Privacy Conference, 2015.

International Organization for Standardization (ISO). 2011. *ISO/IEC 29100: Information technology - Security techniques - Privacy framework.*

Johannesson, Paul & Perjons, Erik. 2014. *An Introduction to Design Science*. Kista: Springer. E-bok.

Koops, Bert-Jaap., Leenes, Ronald. 2013. *Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*. Nederländerna: Tilburg University.

Kroener, Inga., Wright, David. 2014. *A Strategy for Operationalizing Privacy by Design.* I The Information Society, 355–365, 2014. doi: 10.1080/01972243.2014.944730.

National Institute of Standards and Technology (NIST). 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*.

Organisation for Co-operation and Development (OECD). [u.å]. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*..OECD. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (Hämtad 2017-06-09).

Rubinstein, Ira S., Good, Nathaniel. 2013. *Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents*. New York University Public Law and Legal Theory Working Papers. 28 (2). 1334-1414.

Siljee, Johanneke. 2015. *Privacy Transparancy Patterns*. I Proceedings of the 20th European Conference on Pattern Languages of Programs, 2015, Kaufbeuren. New York: ACM.

Solove, Daniel J. 2004. *The digital person: Technology and privacy in the information age*. New York: NyU Press. E-bok.

Spiekermann, Sarah. 2012. *The challenges of privacy by design*. I Communications of the, 38-40, 2012. New York: ACM. doi: 10.1145/2209249.2209263.

Stark, Luke., King, Jen., Page, Xinru., Lampinen, Airi., Vitak, Jessica., Wisniewski, Pamela. 2016. *Bridging the Gap between Privacy by Design and Privacy in Practice*. I Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, 3415-3422, 2016, Santa Clara. New York: ACM.

Vetenskapsrådet. 2011. *God forskningsed*. Stockholm: Vetenskapsrådet.

Bilaga 1: Reflektionsdokument

Reflektionsdokument 1: Lukas Grönquist

Hur svarar Ditt examensarbete mot målen för examensarbetskursen? Varför? Fokusera på de mål som uppfyllts särskilt väl samt de mål som uppfyllts mindre väl.

Hur fungerade planeringen för examensarbetet? Vad hade kunnat göras bättre?

Examensarbetet uppfyller samtliga lärandemål för kursen. Arbetet är skrivet självständigt där den enda utomstående som bidragit till uppsatsens upplägg är handledaren som har handlett oss under arbetets gång. Valet och tillämpningen av vetenskapliga metoder gjordes genom en överläggning mellan författarna, där olika metoder diskuterades och övervägdes för att sedan mynna ut i valen av kartläggning, dokumentstudier och innehållsanalys.

Redan under förra läsåret hade ämnet för uppsatsen beslutats, detta gjorde att sökandet av litteratur för uppsatsen påbörjades redan då. Mycket av litteraturen som togs fram under denna period är den som har refererats till i arbetet. Under tiden på Knowit Secure AB fick vi sedan en vidare konsultation gällande relevant och vedertagen dokumentation inom branschen för it- och informationssäkerhet. Under utförandet har den framtagna litteraturen analyserats genom en innehållsanalys där etiska och samhälleliga aspekter har övervägts under tillämpningen.

Arbetet har sedan presenterats genom en muntlig och visuell presentation vilket lade grunden för oppositionen. Presentationen la grunden för en givande opposition, vilket troligen är det mål som uppfyllts mindre väl då samtliga oppositionsdeltagarna var överens om uppsatsen förbättringsområden. Då deltagarna var överens krävdes inget större försvar. Däremot fick vi möjlighet att förklara och diskutera vad som låg bakom förbättringsområden.

Planeringen var något som till en början av arbetet gick väldigt bra, däremot arbetade vi båda parallellt under arbetets gång. Det parallella arbetet var något som i vissa skeden av ledde till avvikelser i planeringen, detta är något som hade kunnat göras bättre genom att planera det parallella arbete mer i detalj utefter de deadlines som fanns i examenskursen.

Det slutgiltiga arbetet har lett till många nya kunskaper och insikter som sedan har kunnat appliceras i det parallella arbetet med informationssäkerhet.

Om Du utförde examensarbetet tillsammans med en annan student, hur fördelade ni arbetet? Hur fungerade samarbetet? Reflektera också över hur självständigt arbetet genomfördes.

Studenten som jag skrev arbetet med har jag skrivit många uppsatser med och vi är sedan en lång tid tillbaka goda vänner. Detta resulterade i att samarbetet fungerade väldigt bra, då vi vet inom vilka områden vi kompletterar varandra. Detta avspeglades i att vissa delar av arbetet delades upp utefter respektives erfarenheter och kunskaper, medan vissa avsnitt skrevs tillsammans. Allt arbete som har skrivits individuellt har sedan kvalitetssäkrats och ifrågasatts av den andra för att generera en jämn nivå på arbetet.

Då arbetet har pågått iterativt under ett antal månader har vi båda varit delaktiga i mer eller mindre varje mening i uppsatsen, där förbättringar har gjorts kontinuerligt under arbetets tid.

Hur relaterar examensarbetet till Din utbildning? Vilka kurser och områden har varit mest relevanta för examensarbetet?

Då arbetes resultat innehåller såväl administrativa som mer tekniska åtgärder har många delar av utbildningen kommit till användning. Detta då te tekniska åtgärderna som tagits fram genomsyras från diverse tidigare it-relaterade kurser. De kanske främsta kurserna som har varit relevanta för arbetet har varit praktikkursen och de säkerhetsrelaterade kurserna jag har läst. Under säkerhetskurserna fick jag en bred grundkunskap inom området för säkerhet, medan jag under praktiken på Knowit Secure hade möjlighet att ta dessa kunskaper till praktiken. Den tidigare erfarenheten inom området resulterade i mycket av det som arbetet inkluderade var bekant sedan tidigare.

Även kurserna för vetenskapligt skrivande och metod har varit väldigt givande för att kunna genomföra studien.

Hur värdefullt är examensarbetet för Ditt framtida arbete och/eller studier?

Examensarbetet har visat sig vara väldigt värdefullt för mitt framtida arbete, detta då arbetet delvis ledde till en anställning på Knowit Secure AB. Att skriva arbetet i samråd med Knowit Secure ledde till ytterligare möjligheter utöver anställningen, bland annat chansen att presentera studiens resultat på säkerhetskonferens under sommaren 2017.

Vid sidan av examensarbetet har jag även arbetet inom projekt inom nya dataskyddsförordningen, i det projektet har jag kunnat återanvända mycket av kunskapen som genererats i samband med skrivandet av examensarbetet. Erfarenheter inom området för inbyggd integritet och dataskyddsförordningen har också visat sig vara väldigt efterfrågat på arbetsmarknaden, vilket leder till att den vunna kunskapen kommer att hjälpa mig i mitt framtida arbete på Knowit Secure.

Hur nöjd är Du med genomförandet och resultatet av examensarbetet? Varför?

Jag är väldigt nöjd med genomförandet och resultatet av examensarbetet, det var från början ett ämne jag hade låg kunskap inom men som efter arbetet har lett till många nya kunskaper och insikter. De nya kunskaperna är även sådant som jag kommer ha stor nytta av i framtida arbeten inom informationssäkerhet.

En påverkande faktor till att jag är så pass nöjd med arbetet är resultatet som har visat sig vara väldigt efterfrågat, vi ska både presentera det både internt på Knowit men även säkerhetskonferensen CSA Nordic Summit under sommaren.

Jag är även väldigt nöjd med är att vi faktiskt lyckades med att ta det teoretiska konceptet till mer praktiska åtgärder, något som har visats varit väldigt eftertraktat- både i tidigare forskning och i organisationer.

Reflektionsdokument 2: Tobias Rydberg

Hur svarar Ditt examensarbete mot målen för examensarbetskursen? Varför? Fokusera på de mål som uppfyllts särskilt väl samt de mål som uppfyllts mindre väl.

Examensarbetet skulle jag säga uppnår samtliga mål för examensarbetskursen. Arbetet har under dess gång skrivit självständigt där ingen hjälp utöver handledarens feedback har tagits emot. Gällande relevanta vetenskapliga metoder vägdes för och nackdelar med olika metoder för att genom detta fatta ett beslut om vilken metod som var mest lämplig för just detta arbete. Etiska aspekter har även övervägts under hela arbetet, både vid metodval och tillämpning. Då examensarbetet bestod av en dokumentstudie har flera urval gjorts av litteratur där den mest relevanta litteraturen sedan har analyserats och sammanfattats. Detta gjordes även för att titta på tidigare forskning inom området, där denna forskning sattes i förhållande och analyserades kritiskt i förhållande till vår studie. Gällande kunskapsutveckling tycker jag att detta arbete har varit mycket givande, då vi under arbetets gång har fått mycket nya och relevanta insikter inom området som sedan kan applicerats i arbetslivet.

Är det något som kunde ha gjorts bättre så skulle detta nog vara vårt försvarande under oppositionen. Feedbacken vi fick under denna var svår att försvara, och det hade därför nu i efterhand varit bättre om vi varit mer förberedda för denna feedback redan från början. Jag tror att man under uppsatsens gång har blivit lite hemmablind, och tagit vissa delar av uppsatsen för givet, när de i själva verket kan vara svårt att sätta sig in i om man inte är bekant med området sedan tidigare. Detta är något vi kunde ha tänkt mer på under uppsatsens gång, att vara mer tydliga med vad vi menar.

Hur fungerade planeringen för examensarbetet? Vad hade kunnat göras bättre?

Planeringen för arbetet tycker jag har fungerat bra, men hade till viss del kunnat göras bättre. Då både jag och min partner för uppsatsen arbetade parallellt med examensarbetet kunde det vid vissa tillfällen vara så att planeringen mellan arbete och examensskrivande krockade. Detta var något som i sin tur resulterade i att planeringen för arbetet ibland behövde förändras. Något som hade kunnat göras bättre var alltså en bättre planering av det parallella arbetet i förhållande till examensarbetet, för att genom detta förhindra att arbete tog tid från examensarbetet.

Om Du utförde examensarbetet tillsammans med en annan student, hur fördelade ni arbetet? Hur fungerade samarbetet? Reflektera också över hur självständigt arbetet genomfördes.

Samarbetet under examensarbetets gång fungerade mycket bra. Då vi tidigare har gjort andra arbeten tillsammans visste vi sedan innan vad som fungerade bäst för oss när vi jobbade, vilket resulterade i ett effektivt samarbete. Arbetet har sett olika ut beroende på vilken del av uppsatsen som har skrivits, där vi både har delat upp arbetet av denna, samt skrivit andra delar tillsammans. När en uppdelning av arbetet har skett har vi dock varit noggranna med att alltid gå igenom vad den andre personen har skrivit, för att genom detta stämma av med varandra, samt justera efter den andres tycke och tankar. Resultatet av detta har blivit att alla delar i den slutliga uppsatsen i princip är skrivna tillsammans, då vi kontinuerligt och iterativt tillsammans har gått igenom den skrivna texten och gjort justeringar. Arbetet har alltså skett både självständigt samt i par. Att arbeta självständigt har dock inte varit några problem. Då vi arbetat tillsammans sedan tidigare vet vi varandras styrkor, och har därför när det behövts delat upp arbetet efter dessa.

Hur relaterar examensarbetet till Din utbildning? Vilka kurser och områden har varit mest relevanta för examensarbetet?

Då arbetet har utförts inom området för informationssäkerhet har dessa kurser självklart varit relevanta för just detta arbete. Genom SÄK1 och SÄK2 har en grundläggande förståelse och kunskap inom området formats, vilket har varit väldigt hjälpsamt när detta examensarbete har utförts. Utöver detta har även kursen Vetenskapligt skrivande, samt Metod-kursen varit hjälpsamma då jag genom dessa kurser har fått en bättre förståelse för hur en uppsats bör struktureras och skrivas, samt vilka metoder som är mest lämpliga för vilka studier. Utöver detta har jag även under gjort min praktik hos företaget Knowit Secure AB, vilket har resulterat i att en bredare kunskap inom området informationssäkerhet har erhållits. Även detta har varit relevant för examensarbetet, då mycket jag fick göra under praktiken hade någon form av koppling till examensarbetet.

Hur värdefullt är examensarbetet för Ditt framtida arbete och/eller studier?

Då examensarbetet delvis resulterade i en anställning hos Knowit Secure AB, där mycket av arbetet som kommer att utföras berör den nya dataskyddsförordningen är detta arbete något som har varit värdefullt. De åtgärder och lösningar som genom denna studie identifierats är något som kommer att vara användbart i mitt framtida arbete.

Hur nöjd är Du med genomförandet och resultatet av examensarbetet? Varför?

Både resultatet och genomförandet av uppsatsen är något som jag är nöjd över. Jag tycker att ämnet vi under uppsatsens gång har behandlat har varit mycket intressant, och att arbetet i sin helhet har varit givande att utföra. Då resultatet av detta arbete är något jag kan ta med mig in i arbetslivet är detta även något jag är nöjd över, då det utöver den kunskap som erhållits under arbetets gång faktiskt även kan få en praktisk tillämpning.

Stockholms universitet
Institutionen för data- och systemvetenskap
Borgarfjordsgatan 12
SE-164 07 Kista
Telefon/Phone: 08 – 16 20 00
www.dsv.su.se