LUNDS UNIVERSITET
Ekonomihögskolan

Informationssäkerhet vid tredjelandsöverföringar

Kandidatuppsats 15hp, SYSK02 i Informatik
Framlagd: 2013-06-05
Författare: Henrik Georgson och Emil Kristiansson
Handledare: Anders Svensson
Examinatorer: Paul Pierce och Markus Lahtinen

Abstrakt

Titel:	Informationssäkerhet vid tredjelandsöverföringar
Författare:	Henrik Georgson och Emil Kristiansson
Utgivare:	Institutionen för Informatik, Lunds Universitet
Handledare:	Anders Svensson
Examinatorer:	Paul Pierce och Markus Lathinen
Publiceringsår:	2013
Uppsatstyp:	Kandidatuppsats
Språk:	Svenska
Nyckelord:	Dataskyddsförordning, Informationssäkerhet, personuppgifter, tredje land, datadirektiv

Syftet med den här uppsatsen har varit att undersöka hur EU-kommissionens förslag till ny dataskyddsförordning kan komma att påverka informationssäkerheten vid överföringar av personuppgifter till ett tredjeland. Detta har gjorts genom att studera hur de nuvarande lagarna ser ut för att sedan jämföra de med förslaget. Utöver detta har vi studerat hur organisationer kan förhålla sig till informationssäkerhet genom att använda olika modeller, metoder och best practise-lösningar. På så vis har vi kommit fram till hur de kan upprätthålla en bra skyddsnivå. För att sätta in oss i detta har vi haft ett företag som studieobjekt som vi har hämtat exempel ifrån.

För att komma fram till ett relevant och riktigt resultat har vi genomfört fyra kvalitativa intervjuer med personer som besitter olika kompetenser. Utöver de källorna har vi använt oss av litteratur och även till viss del media för att skapa oss en bild av den aktuella debatten.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Inom informatikämnet berörs en rad olika områden vars gemensamma nämnare är att alla innefattar IT och människor på olika sätt. Ett av dessa områden innefattar lagar och regler som berör ämnet ur ett juridiskt perspektiv, vilket bygger på den rådande lagstiftningen och hur företag anpassar sig för att följa den. För att förstå och kunna jobba med informationssäkerhet måste det finnas kunskap om hur de aktuella lagarna interagerar och förhåller sig till informatik.

Begreppet outsourcing har i dagens globaliserade värld blivit en familjär term. Inom IT-branschen betyder outsourcing att en organisation (exempelvis den offentliga sektorn eller ett privat företag) låter ett IT-företag ta hand om hela eller vissa delar av organisationens IT-miljö och behovet av egen IT-personal minskar därmed. Nästa steg är att IT-företaget strävar efter att hålla nere sina kostnader för utveckling av exempelvis nya system och därför är intresserade av arbetskraft i ett land med lägre löner. Detta kallas då för offshoring. I samband med begreppet offshore, då det rör organisationer verksamma inom EU och EES, talas det om ”tredje land” och då avses ett land som är utanför EU och EES.

IT-företagens kunder kan i sina verksamheter exempelvis hantera och lagra personuppgifter, vilket skapar ett stort ansvar gentemot individen. Enligt personuppgiftslagen (PUL) blir då IT-företagen personuppgiftsbiträde (SFS 1998:1191). Om uppgifterna hamnar i orätta händer kan det leda till allvarliga konsekvenser för alla inblandade personer. För att den enskilda individen ska känna en tillförlitlighet för att dess personuppgifter hanteras korrekt finns juridiska restriktioner med syfte att säkerställa detta.

Idag finns det ett dataskyddsdirektiv från 1995 som gäller för länderna i EU och EES (EU: Dataskyddsdirektivet). På detta bygger PUL som trädde i kraft 1998, och talar om hur personuppgifter får lagras och hanteras för att kunna garantera säkerhet gentemot den enskilda individen (DI: Personuppgiftslagen). Då IT-branschen ständigt utvecklas, i hög takt, har det därför blivit aktuellt med en ny förordning.

Det är viktigt att förstå skillnaden mellan direktiv och förordning. En förordning blir direkt gällande i alla EUs medlemsstater och blir på så sätt en form av lag (EU: Förordningar och direktiv). Ett direktiv är något svagare och fungerar som ett mål som länderna bör försöka uppnå. Notera att EU-kommissionen nu vill ersätta ett direktiv med en förordning.

PUL begränsar organisationers rätt att behandla personuppgifter i ett tredje land. Det finns dock två undantag:

- EU tillhandahåller en lista över länder som anses upprätthålla en adekvat skyddsnivå.

- Den registeransvarige får sluta ett avtal med en tredje man om att de upprätthåller en tillräckligt hög skyddsnivå av uppgifterna.

Till det nuvarande direktivet finns det standardavtalsklausuler som används mellan två parter för att sluta ett juridiskt bindande avtal om att personuppgifterna behandlas korrekt i ett tredje land (DI: Standardavtalsklausuler). Dessa två parter kan alltså vara en organisation och ett IT-företag som samarbetar som kund och leverantör. Klausulerna definierar vilka, hur och när personuppgifter får behandlas i ett tredje land. Genom de här klausulerna får IT-företaget därmed möjlighet att behandla alla eller vissa delar av personuppgifterna i ett tredje land.

Då detta fortfarande bara är ett förslag är det ett begränsat antal personer som är införstådda i vad det kan komma att innebära för svenska organisationer (Computer Sweden: debatt, 2013). Det har dessutom inte uppstått någon större debatt kring förslaget i Sverige ännu vilket ytterligare försvårar arbetet med att sätta sig in i vilka konsekvenser införandet av en ny förordning innebär för IT-branschen.

Företaget som är objekt för den här studien har valt att vara anonymt och kallas hädanefter för Heit. Heit är ett större globalt IT-företag som är en helhetsleverantör av lösningar och tjänster till flertalet branscher. Lösningarna och tjänsterna är såväl affärskritiska som samhällskritiska och därför står säkerhet och kvalitet högt på företagets agenda.

Heit finns med cirka 20 000 anställda representerade i ett tjugotal länder i Europa, Nordamerika och delar av Asien. En av Heits grundtjänster är outsourcing, med offshoring som en viktig del för att möta kundernas behov och den starka konkurrens som finns på marknaden. När vi kom i kontakt med Heit var de därför intresserade av att veta hur de kan komma att påverkas om den nya förordningen träder i kraft.

1.2 Problemområde

I dagens samhälle har outsourcing blivit en allt vanligare affärsmodell (Handsfield R, A Brief History of Outsourcing 2006). Detta innebär att allt fler organisationer har släppt kontrollen över sin information men då de fortfarande är ansvariga för den information de har uppstår ett problem. Samtidigt som organisationer lägger över ansvaret på någon annan måste de kontrollera att de följer de lagar som finns. När en organisation hanterar personuppgifter finns det en särskild lag som måste följas, nämligen PUL. När det nu har blivit aktuellt med en ny lagstiftning som ska skapa en ökad harmonisering inom EU måste både organisation som är ansvariga för personuppgifter och IT-företagen sätta sig in i vad som gäller i framtiden. Vi kommer därför undersöka hur den nya lagstiftningen kan komma att påverka IT-branschen vid överföring av personuppgifter till tredje land.

1.3 Forskningsfråga

Hur kommer ett personuppgiftsbiträde (eller registerförare som det kallas i förslaget, se 1.1) att behöva anpassa sina offshoreåtaganden om EU-kommissionens förslag till ny dataskyddsförordning träder i kraft i sin nuvarande form?

1.4 Syfte

Syftet med den här studien är att ta reda på hur IT-branschens arbete med outsourcing till ett tredje land kan komma att påverkas om förordningen träder i kraft i linje med det förslag som finns. Vi vill att den här studien ska kunna användas som underlag när det blir aktuellt att anpassa arbetet utifrån den nya förordningen.

1.5 Avgränsningar

Förslaget är omfattande och kan påverka hanteringen av personuppgifter på en mängd olika sätt. I förslaget finns det t.ex. nya krav på hur den registrerade ska ha rätt att bli glömd och även kunna föras över till andra system. Vi har dock valt att enbart studera de delar i förslaget som direkt påverkar arbetet med överföringar av personuppgifter till tredje land.

2 Litteraturgenomgång

2.1 Begrepp

För att förstå och därmed kunna sätta sig in i den aktuella lag och det aktuella förslaget finns det ett antal centrala begrepp som är viktiga att ha kunskap om. Eftersom dessa inte lämnar något utrymme för tolkning har vi valt att ta med dem i sin helhet från förslaget till förordningen.

- *den registrerade*: ’’ en fysisk person som är direkt eller indirekt identifierad eller identifierbar, med medel som rimligen kan komma att användas av den registeransvarige eller av någon annan fysisk eller juridisk person, framför allt med hänvisning till ett identifikationsnummer, en lokaliseringsuppgift eller nätidentifierare, eller till en eller fler faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet” (COM(2012) 11 Final 2012/0011 (COD))

- *personuppgifter*: ”Varje upplysning som avser den registrerade.” (COM(2012) 11 Final 2012/0011 (COD))

- *behandling*: ’’varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, radering eller förstöring” (COM(2012) 11 Final 2012/0011 (COD))

- *register:* ’’varje strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden” (COM(2012) 11 Final 2012/0011 (COD))

- *registerförare:* ’’en fysisk eller juridisk person, myndighet, institution eller annat organ som behandlar personuppgifter för den registeransvariges räkning” (COM(2012) 11 Final 2012/0011 (COD))

- *Registeransvarig*: ’’avser samma som *personuppgiftsansvarig*, en fysisk eller juridisk person, myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen, villkoren och medlen för behandlingen av personuppgifter; om ändamålen, villkoren och medlen för behandlingen bestäms av unionslagstiftningen eller medlemsstaternas lagstiftning kan den registeransvarige

eller de särskilda kriterierna för hur denne ska utses anges i unionslagstiftningen eller i medlemsstaternas lagstiftning" (COM(2012) 11 Final 2012/0011 (COD))

- *Tredje man*: ''Tredje man är den person, fysisk eller juridisk, som utan att vara part berörs av en rättshandling eller en tvist." (COM(2012) 11 Final 2012/0011 (COD))

- *Personuppgiftsbrott:* "ett säkerhetsbrott som leder till förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats" (COM(2012) 11 Final 2012/0011 (COD))

- Tredje land: ''Ett så kallat tredje land är ett land som inte är medlem i EU eller EES'' (DI: tredjeland)

2.2 Säkerhet

Säkerhet är ett begrepp som kan syfta på en rad olika saker och därmed tolkas på många sätt. Vi tar här upp några olika synsätt och teorier som vi bedömer relevanta för den här studien.

2.2.1 Informationssäkerhet

I dagens organisationer är det viktigare än någonsin att skydda organisationens information. Vi anser att innan vi börjar prata om IT-säkerhet behövs en förståelse för vad informationssäkerhet inom en organisation är. För att IT-användningen ska vara säker och korrekt krävs det fungerande säkerhetsrutiner även utanför IT-avdelningen.

Andress (2011, The Basics of Information Security, s. 2) menar på att säkerhet är att skydda våra tillgångar. Skyddet kan vara såväl fysiskt skydd mot naturkatastrofer som en brandvägg som skyddar mot intrång på nätverket. Val av skydd beror givetvis på vad som ska skyddas. Han menar även att det normalt sett är personer som är den viktigaste tillgången eftersom organisationen inte fungerar överhuvudtaget utan personer som utför olika uppgifter.

Vidare menar Andress (2011, s. 2-3) att hänsyn måste tas till hur säkerheten påverkar användbarheten. Med andra ord innebär det att ett helt säkert system förmodligen inte går att använda alls. Sedan finns det även en ekonomisk aspekt. Frågan som måste besvaras är hur mycket pengar det är värt att lägga ner i att säkra den aktuella tillgången.

Enligt Bunker (2011, Technology is not enough: Taking a holistic view for information assurance, s. 19) har informationssäkerhet blivit ett hett ämne inom hela organisationen, även för styrelsen. Detta beror delvis på den mänskliga faktorn, som vi går igenom senare, men också p.g.a. att allt mer information lagras elektroniskt. På så sätt kan konsekvenserna av en attack eller borttappad enhet bli större och allvarligare för organisationen.

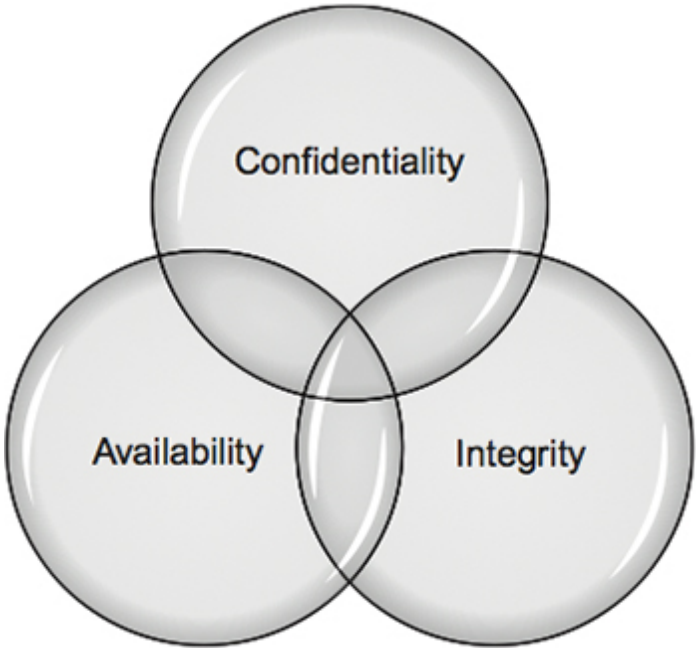
Ytterligare en aspekt som organisationen måste ta hänsyn till är lagar och regler när det blir allt vanligare med s.k. molnlösningar där informationen lagras hos en IT-leverantör. Det uppstår då ett beroende som inte existerade för ett par decennier sedan (Bunker 2011, s. 24).

Det är vanligt att organisationen inte har koll på var informationen fysiskt lagras. Därmed blir det svårt eller omöjligt att kontrollera att policys, lagar och regler efterföljs på ett korrekt sätt. Om en organisation använder sig av molnlösningar är det viktigt att dess säkerhetspolicys är uppdaterade så att de går att applicera på en molnmiljö. Det är även viktigt för en organisation att tillhandahålla träning och utbildning, att se till att IT-avdelningen är införstådda med problematiken och att organisationen går igenom vilka molnleverantörer som är pålitliga och därmed får användas (Bunker 2011, s. 24).

Bunkers (2011, s. 19) lösning på detta är att ha en holistisk syn på informationssäkerhet och på så sätt skapa sig en bild av hur organisationen jobbar med information från olika perspektiv. Detta kan även leda till lägre kostnader och konkurrensfördelar om det utförs på ett bra sätt.

2.2.2 Konfidentialitet, integritet och tillgänglighet

Det finns som sagt många sätt att förhålla sig till informationssäkerhet och för att få en övergripande bild när olika problem diskuteras kan det enligt Andress (2011, s. 4) vara bra att använda sig av en modell. En av många modeller som han nämner är CIA-triangeln. CIA står för Confidentiality, Integrity och Availability vilket fritt översatt blir konfidentialitet, integritet och tillgänglighet.



Figur 2.1, CIA-triangeln (Andress s. 5 2011)

Konfidentialitet
Med begreppet konfidentialitet menar Andress (2011, s. 4) att informationen ska vara skyddad på ett sådant sätt att obehöriga inte kommer åt den och att konfidentialitet existerar på många olika nivåer i en process. Vidare menar han att det kan röra sig om allt från att en obehörig person ser när ett lösenord slås in till att någon stjäl en laptop eller att någon hackar sig in i ett system.

Integritet
Integritet innefattar ett skydd mot att uppgifter i exempelvis ett system blir felaktigt ändrade, antingen av en obehörig person eller av misstag, enligt Andress (2011, s. 5). För att skydda sig mot detta måste det finnas möjlighet att återskapa borttagen information. Andress menar att det kan få förödande konsekvenser om kritisk information ändras på ett felaktigt sätt, i värsta fall skulle det rent av kunna leda till att en patient dör om det handlar om information inom ett sjukhus.

Tillgänglighet
För att exempelvis ett system ska vara säkert menar Andress (2011, s. 6) att det är oerhört viktigt att det är tillgängligt när det behövs. En systemkrasch kan orsaka stora skador för de som är beroende av systemet vilket i förlängningen innebär att både förtroende och pengar förloras.

CIA-triangeln är applicerbar på en mängd olika situationer och på olika nivåer. Andress (2011, s. 6) nämner som ett exempel att om band används för backup går det att göra en analys med hjälp av CIA-triangeln på hur säker lösningen är. Frågor som då kan uppstå är hur det exempelvis är krypterat. Med andra ord kan en mängd olika problem lyftas fram och förhoppningsvis lösas. På så sätt uppnås en relevant helhetsbild.

2.2.3 Best practise

I artikeln "Best practices for security and controls for corporate treasurers" skriver Sally Hart (2010) om olika metoder för ekonomisk säkerhet i organisationer, men vi tycker att den går att tillämpa till stora delar även på informationssäkerhet inom organisationer. Hart (2010, s. 353) menar att en organisation först och främst måste sträva efter transparens och riskmedvetenhet, samt se till att olika best practiselösningar följs. På så sätt undviks många risker på olika plan i organisationen.

Policys
Hart (2011, s. 354) menar att det viktigaste att göra är skapandet av en komplett uppsättning av policys som täcker in de berörda områdena. Policyerna ska vara enkla, tydliga och lätta att förstå. Personerna som tar fram de olika policyerna bör vara seniora och ha mycket erfarenhet, därefter ska policyerna godkännas av styrelsen. Det blir sedan chefernas ansvar att de anställda tar del av policyerna och styrelsen har ansvar för att se över att de efterföljs.

Även Petlier (2005, Information Security Fundamentals) menar på att det är väldigt viktigt med välutformade policys för att skydda informationen i en organisation. Han menar även på att det finns både interna och externa syften med policys. Genom att ha policys kan en högre skyddsnivå uppnås internt och detta leder till att organisationen kan gå ut och försäkra kunder och resten av omvärlden om att de upprätthåller en hög skyddsnivå.

Administrativa kontroller och procedurer
För att policyerna ska kunna efterföljas måste det finnas olika begränsningar och kontroller. Dessa kan både vara tekniska, automatiska eller manuella. Det kan med andra ord innebära begränsningar för en användare i ett system eller att en person inom organisationen granskar en annan persons arbete (Hart 2011, s. 354).

Uppdelning av uppgifter
Genom att se till att en person inte kan göra kritiska uppgifter utan att en annan person godkänner det i slutet av processen ökar säkerheten markant. Det går inte att komma från att det ofta är den mänskliga faktorn i sig som är den största säkerhetsrisken, något vi återkommer till senare. I artikeln tas det som ett exempel upp att en person inte ska kunna göra ett inköp utan att någon annan kontrollerar och godkänner det (Hart 2011, s. 355).

Rapportering
Det sista Hart (2011, s. 356) tar upp i sin artikel är vikten av att ha en fungerande rapportering inom organisationen. På så sätt ökar medvetenheten hos de seniora ledarna och misstag kan identifieras, både på kort och lång sikt. Rapporterna bör i största möjliga mån vara genererade direkt i ett system för att minska risken för att någon människa går in och förändrar information till sin egen förmån.

2.2.4 Accountability och auditing

Det är viktigt att personer som kommer i kontakt med känslig information förstår vilket ansvar det innebär, vilket även måste kontrolleras (Andress 2011, s. 51). Med andra ord räcker det inte med en mängd olika tekniska säkerhetsfunktioner. De är i själva verket bara hjälpmedel för att upprätthålla en hög säkerhetsnivå.

Accountability
Andress (2011, s. 52) menar på att en ansvarskänsla kan skapas hos personer genom att kontrollera vad de gör. Personer som är medvetna om att de kontrolleras på olika sätt är mer måna om att göra rätt. Det är dock viktigt att kontrollerna inte går till överdrift. Det finns en mängd olika fördelar med att skapa en ansvarskänsla genom t.ex. att personer kan hållas ansvariga för sina handlingar, samt att genom övervakning upptäcka intrång och andra attacker i ett tidigt skede (Andress 2011, s. 55).

Auditing
Auditing är bland annat ett tekniskt hjälpmedel för att skapa accountability. Det finns flera olika tillvägagångssätt och en uppsjö av olika tekniska plattformar. Andress går igenom några

(2011, s. 57-58). Ofta är det lagar och regler som ställer krav på att dessa tekniska lösningar ska finnas, men även organisationens intresse att skydda sina företagshemligheter skapar en efterfrågan. En av de vanligaste metoderna vi kommer i kontakt med är lösenord, men det finns även långt mer avancerade metoder. En vanlig lösning som ofta ställer högre krav på den tekniska plattformen är loggning, vilket helt enkelt innebär att vem som gör vad sparas i systemet. På så sätt finns det möjlighet att gå tillbaka och se vad som har skett när och vem som har utfört åtgärden. Nästa steg är övervakning av exempelvis olika resurser. Det leder till att onormala aktiviteter kan upptäckas, som att trafiken på nätverket plötsligt ökar till onormala nivåer. Det finns även olika sätt att testa sina system för att mäta säkerheten. Ett exempel på detta är att göra s.k. penetrationstest där säkerheten analyseras och mäts genom att simulera en attack. Dessa kan utföras med enkla medel men också av ett företag som specialiserat sig på säkerhet.

2.2.5 Den mänskliga faktorns roll inom IT-säkerhet

IT-säkerhet är för de flesta förknippat med tekniska begrepp så som brandväggar, lösenord, krypterade filer och VPN-tunnlar. Verkligheten ser dock ut som sådan att de flesta säkerhetsincidenterna har berott på okunskap hos människor. Det finns åtskilliga exempel på hur sådana incidenter kan se ut. Det kan vara att en person på en arbetsplats lånar en kollegas lösenord som sedan hamnar i orätta händer. Man kanske jobbar på en privat dator som innehåller virus som på så sätt tar sig in i jobbets maildatabas. Det kan också vara att man glömmer ett USB-minne med konfidentiell information som hamnar i orätta händer. Detta är några exempel på hur säkerheten kan rubbas p.g.a. av den mänskliga faktorn(Gregory 2003, Enterprise Information security, s 93 -102).

Det enklaste sättet att motarbeta att sådana här situationer inträffar är att se till att agera i förebyggande syfte. Det kan göras genom att ha utbildningar där ett riskmedvetande tänk lärs ut. Arbetsplatser där de anställda jobbar hemifrån är ett bra exempel där det är extra viktigt med sådana utbildningar. Det kan nämligen innebära att datorn som är avsedd för arbete även används för privat bruk så som att läsa privata mail eller surfa på internet (Thompson 2013, The human Element of information security s. 32-35).

Kontentan är att IT-säkerhet inte är ett rent tekniskt begrepp som handlar om att skydda sin data med hjälp av speciella säkerhetsprogram utan om att det först och främst är något som styrs och påverkas av människors godtrogenhet och okunskap. Att utbilda människorna i en organisation till att förstå vad konsekvenserna av olika handlingar kan leda till och öka riskmedvetandet hos är en nyckelfaktor när det kommer till IT-säkerhet (Thompson 2013, s. 32-35).

2.3 Kvalitetssäkring

För att bygga ett förtroende både internt och externt är det viktigt för en organisation att kunna påvisa att deras produkter och tjänster håller en hög kvalitet. Detta kan påvisas genom

att organisationen certifierar sig inom olika områden och då kommer olika ISO-standarder in i bilden.

2.3.1 ISO 9001

ISO 9001 är en kvalitetsstandard som utgår från åtta principer. Dessa används som ett ramverk för att kunna leda en hel organisation mot förbättring. När dessa har utformats så har de baserats på erfarenhet och kunskap (ISO Central Secretariat 2012, Quality management principles). De åtta principerna är kundfokus, ledarskap, involvera människor, processansats, systemansats mot ledningen, fortsatt förbättring, faktisk ansats och gemensamma fördelar i leverantörsrelationer.

Kundfokus
Organisationer är beroende av sina kunder, både nuvarande och framtida, och ska därför se till att tillgodose deras krav och förväntningar.

Ledarskap
Ledare definierar organisationens syfte och riktning. På så sätt skapas en miljö som alla människor involverade i organisationen verkar i.

Involvera människor
Människor, på alla nivåer, är det primära i organisationen och ju mer de involveras ju mer fördelar kan de skapa åt organisationen.

Processansats
Ett bestämt mål är enklare att nå om aktiviteter och resurser ses som processer.

Systemansats mot ledningen
Att identifiera, förstå och leda interna processer inom organisationen kommer leda till förbättring och effektivitet.

Fortsatt förbättring
Det bör hela tiden finnas ett mål inom organisationen att förbättra den totala prestationen.

Faktisk ansats mot förbättring
Effektiva beslut baseras på analyser av data och information.

Gemensamma fördelar i leverantörsrelationer
Både organisationen och dess leverantörer är beroende av att samarbeta för att uppnå bästa möjliga resultat

Detta är en kort sammanfattning av det ramverk som används när ISO 9001 tillämpas. En implementering baserat på dessa principer leder till effektiva förbättringar på hela organisationen (ISO Central Secretariat 2012, Quality management principles).

2.3.2 ISO 27001

ISO 27001 är en en säkerhetsstandard som används för att en organisation ska kunna säkerställa att känsliga uppgifter hanteras på ett korrekt sätt så att den personliga integriteten skyddas. ISO 27001 bygger på en modell som innefattar en rad steg som tillämpas på säkerhetssystemet: etablera, implementera, verka, övervaka, granska, upprätthålla och förbättra (Gillies 2011, Improving the quality of information security management systems with ISO 2700, s 367-376).

Standarden är en generell lösning som kan tillämpas på all sorts data. Det vill säga både digital och fysisk samt medarbetares olika kunskaper. Med andra ord så skyddar standarden för alla möjliga scenarier oavsett om det är brand i ett serverrum, ett intrång från en hackergrupp eller att en anställd råkar nämna konfidentiell information på en allmän plats (DNVBA: Vad är ISO 27001?).

2.4 Nuvarande lagstiftning

2.4.1 Personuppgiftslagen

Personuppgiftslagen (PUL) verkställdes 1998 med syfte att garantera skydd gentemot den personliga integriteten och behandling av personuppgifter (SFS 1998:204). Detta utarbetades utifrån datadirektivet och bygger på regler som beslutats och utformats inom EU vilket innebär att olika motsvarigheter till PUL förekommer inom de olika länderna i EU. PUL utgår främst från den enskilda individens samtycke till hur dennes personuppgifter ska behandlas.

Överföring av personuppgifter till tredje land
I PUL finns det tre paragrafer som är intressanta för den här studien då de behandlar överföring till tredje land. Nedan följer en kort beskrivning av de för oss intressanta paragraferna.

I 33§ förbjuds överföring och behandling till tredje land om landet inte har en adekvat skyddsnivå (SFS 1998:204).

Det finns dock möjlighet till undantag i vissa fall som beskrivs i 34§. Om den registrerade ger sitt samtycke får en överföring eller behandling i tredje land ske. Det kan även bli tillåtet om exempelvis “vitala intressen för den registrerade skall kunna skyddas” (SFS 1998:204).

35§ klargör att undantag är tillåtna om det finns ett avtal som garanterar att tillräckligt skydd för den registrerade. Ett sådant avtal ska dock först godkännas av regeringen (SFS 1998:204).

Påföljder
I 49§ står det att den som bryter mot PUL kan dömas till böter eller fängelsestraff i högst sex månader. Om brottet är grovt kan det bli två års fängelsestraff och brottet anses grovt

exempelvis om uppgifter överförs till ett land som inte tillhandahåller en adekvat skyddsnivå (SFS 1998:204).

Vi har inte funnit några rättsfall där böter har dömts ut.

2.4.2 Personuppgiftsförordningen

Till PUL finns ett komplement i form av personuppgiftsförordningen. I förordningen beskrivs en del bestämmelser mer i detalj och det som är intressant för den här studien är en paragraf som behandlar överföring av personuppgifter till tredje land.

I 13§ slås det fast att det är tillåtet med en överföring till ett tredje land om EU-kommissionen har fastställt att landet har adekvat skyddsnivå eller om personuppgifterna förs över med skydd av ett avtal som innehåller standardavtalsklausuler fastställda av EU-kommissionen. Datainspektionen (DI) är tillsynsmyndighet för dessa frågor och får enligt 14§ även godkänna vissa undantag om det finns tillräckliga garantier (SFS 1998:1191).

2.4.3 Adekvat skyddsnivå

Det är EU-kommissionen som beslutar om ett land har adekvat skyddsnivå eller inte. De bedömer detta utifrån ett antal olika riktlinjer och sedan ska även överföringen vara väl motiverad samt anses nödvändig (DI: adekvat skyddsnivå).

2.4.4 Binding corporate rules

När en företagskoncern har verksamhet i flera länder kan det uppstå ett behov av att flytta personuppgifter om anställda eller kunder inom koncernen. Detta kan tillåtas genom att Binding Corporate Rules (BCR) upprättas och godkänns av berörda tillsynsmyndigheter. Om koncernen är aktiv i flera länder inom EU/EES måste respektive lands tillsynsmyndighet godkänna avtalet för att uppgifter ska få överföras från det aktuella landet. (DI: binding corporate rules)

Ett exempel på en koncern som använder sig av BCR är Hewlett Packard (HP). På deras webbsida klargör de att de har BCR som gäller i de flesta EU/EES-länder och därmed får föra över personuppgifter till ett tredje land. Vidare informerar de om vilka rättigheter den registrerade har och hur den registrerade går till väga om denna har synpunkter eller vill stämma HP (HP - Binding Corporate Rules).

2.4.5 Standardavtalsklausuler

Som vi tidigare nämnde finns det möjlighet att föra över personuppgifter till tredje land om avtalet innefattar standardavtalsklausuler. Klausulerna fastställer hur och vilka personuppgifter som får föras över till ett tredje land. Det framgår även vad den registrerade har för rättigheter samt hur eventuella tvister ska lösas (DI: standardavtalsklausuler).

Vi har sett närmare på ett av dessa tre klausuldokument och här följer en kortare sammanfattning. Dokumentet inleds med en förklaring av varför det behövs och vilka syften som uppfylls. Därefter finns det tolv klausuler som bl.a. förbinder uppgiftsföraren att tillhandahålla tillräckliga säkerhetslösningar. Det är i tillägg 1 som de båda parterna skriver in vad som ska överföras och skriver under på att det finns tillräckliga skyddsåtgärder för att säkerhetsnivån ska anses vara adekvat. I tillägg 2 beskrivs sedan vilka tekniska och organisatoriska åtgärder som har vidtagits (EU: standardavtalsklausul).

2.5 Förslag till ny förordning

2.5.1 Kortfattad genomgång

Det är viktigt att vara medveten om två saker när förslaget till den nya förordningen läses. Dels att det för det första bara är ett förslag som kan komma att ändras innan det röstas igenom, dels att förordningen blir direkt gällande i alla EUs medlemsstater.

Förslaget handlar i största allmänhet om hur personuppgifter får behandlas och det vi kommer att fokusera på här är kapitel fem som handlar om överföring av uppgifter till tredje land. Nedan följer en redogörelse för de artiklar i förslaget som vi har funnit mest intressanta för denna studie.

2.5.2 Artikel 40 - Allmän princip för överföring av uppgifter

I artikel 40 fastställs hur uppgifter får överföras till ett tredje land om de krav som finns i de kommande artiklarna i kapitel fem uppfylls (COM(2012) 11 Final 2012/0011 (COD)).

2.5.3 Artikel 41 - Överföring efter beslut om adekvat skyddsnivå

Det framgår i artikel 41 att en överföring är tillåten om kommissionen har beslutat att landet eller den internationella organisationen uppfyller kraven för en adekvat skyddsnivå. Kommissionen ska också publicera en lista över de länder som inte anses upprätthålla en adekvat skyddsnivå. (COM(2012) 11 Final 2012/0011 (COD))

2.5.4 Artikel 42 - Överföring med stöd av lämpliga skyddsåtgärder

Enligt artikel 42 får överföringar även ske om det inte finns ett beslut i enlighet med artikel 41 om lämpliga skyddsåtgärder har vidtagits genom ett juridiskt bindande instrument. Exempel på juridiskt bindande instrument är BCR, standardiserade uppgiftsskyddsbestämmelser och avtalsklausuler. Dessa redogör vi för senare i detta avsnitt. Det går även att söka tillstånd för en eller en serie överföringar hos tillsynsmyndigheten. (COM(2012) 11 Final 2012/0011 (COD))

2.5.5 Artikel 43 - Överföring med stöd av bindande företagsbestämmelser

Bindande företagsbestämmelser är den svenska översättningen av Binding Corporate Rules som vi tidigare har skrivit om, vi kommer även i fortsättningen kalla det för BCR då det är det vedertagna begreppet. I artikeln fastställs att BCR godkänns automatiskt om de uppfyller

vissa krav. Kraven finns att läsa i 43.2 (COM(2012) 11 Final 2012/0011 (COD)) och det är bl.a.:

- För att de ska godkännas måste den registrerades rättigheter finnas med och samtliga personer i företagsgruppen ska omfattas.
- Vidare måste BCR innehålla information om företagsgruppen samt vilka personuppgifter som kan komma att överföras.
- Det ska även finnas information om hur de registrerade ska informeras och företagsgruppens rutiner för kontroll.

Enligt tredje punkten i artikel 42 (COM(2012) 11 Final 2012/0011 (COD)) ska inga andra tillstånd krävas för att överföringar ska få ske.

2.5.6 Artikel 44 - Undantag

Det finns en mängd olika undantag då en överföring får ske. Ett exempel är att överföring får ske om den registrerade har gett sitt samtycke till överföringen (COM(2012) 11 Final 2012/0011 (COD)). De flesta undantag är dock inte intressanta för denna studie.

2.5.7 Artikel 45 - Internationellt samarbete för skydd av personuppgifter

Artikeln beskriver hur kommissionen och tillsynsmyndigheterna ska utveckla rutiner för att lagstiftningen ska fungera samt ta fram gemensamma skyddsåtgärder (COM(2012) 11 Final 2012/0011 (COD)).

2.5.8 Adekvat skyddsnivå

I 41.2 beskrivs vad kommissionen ska ta hänsyn till när de bedömer om ett land har adekvat skyddsnivå (COM(2012) 11 Final 2012/0011 (COD)). Det är exempelvis om landet har en god allmän säkerhet med bland annat fungerande administration samt oberoende tillsynsmyndigheter för den här typen av frågor. Det tas även hänsyn till hur landets internationella arbete ser ut och fungerar.

2.5.9 Standardavtalsklausuler

I 42.2 c (COM(2012) 11 Final 2012/0011 (COD)) står det:

> "standardiserade uppgiftsskyddsbestämmelser som antagits av en tillsynsmyndighet enligt den mekanism för enhetlighet som avses i artikel 57 förutsatt att denna bestämmelse förklarats allmänt sett giltig enligt artikel 62.1 b"

Standardiserade uppgiftskyddsbestämmelser kan exempelvis vara standardavtalsklausuler. Sedan står det i 42.3 (COM(2012) 11 Final 2012/0011 (COD)):

> "En överföring som grundar sig på standardiserade uppgiftsskyddsbestämmelser eller bindande företagsregler enligt punkt 2 a, b eller c ska inte kräva något ytterligare tillstånd. "

Vilket alltså innebär att det även fortsättningsvis kommer finnas möjlighet att använda sig av standardavtalsklausuler samt att dessa inte måste godkännas av DI.

2.5.10 Påföljder

I kapitel åtta klargörs vilka påföljderna blir om förordningen inte följs. Detta kan leda till böter som fastställs i artikel 79. Straffskalan delas in i fyra steg där det mildaste straffet är en skriftlig varning. Steget därpå innebär böter upp till 250 000 euro eller 0,5% av företagets omsättning. Tredje steget innebär böter upp till 500 000 euro eller 1% av omsättningen och det sista steget innebär böter upp till 1 000 000 euro eller 2% av omsättningen. Varje steg har olika motiveringar och ju grövre överträdelsen är desto högre blir böterna (COM(2012) 11 Final 2012/0011 (COD)).

2.6 Skillnader mellan nuvarande lagstiftning och förslaget

Det kan vara svårt att utan juridisk expertis förutsäga vad det finns för skillnader och vilka av de som kommer bli av störst betydelse för IT-branschen. Vi finner det dock intressant att EU-kommissionen strävar efter att BCR ska förenklas och bli mer användbart genom att bland annat ta bort kravet på att det ska godkännas av en tillsynsmyndighet. Vidare kan vi även konstatera att påföljderna är hårdare än i dagsläget.

2.7 Heits arbete kring informationssäkerhet

Efter att ha studerat vårt undersökta företag arbetssätt gällande informationssäkerhet och överföringar av personuppgifter till tredje land kan vi konstatera att de använder sig av ett för branschen vanligt sätt att jobba på. Detta finner vi eftersom de använder sig av standardavtalsklausuler, certifieringar och har en genomtänkt teknisk lösning för att garantera informationssäkerhet. Det viktiga här är inte en viss teknisk lösning, istället ser vi det som ett exempel på hur ett företag kan hantera information på ett säkert sätt i tredje land.

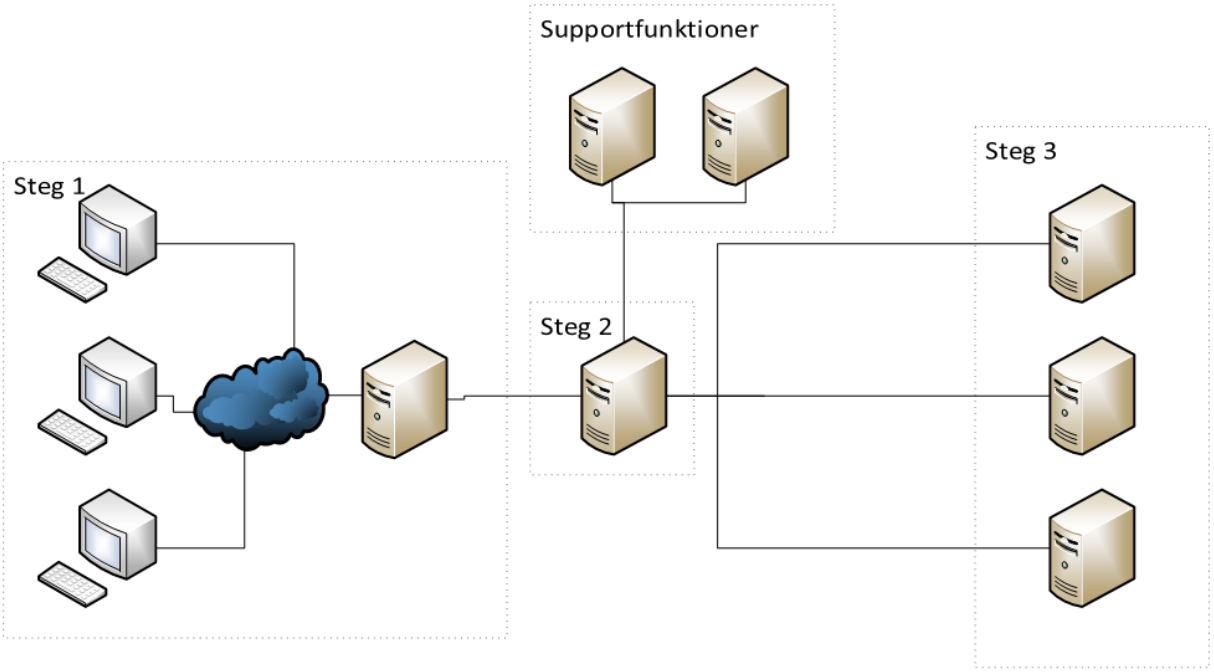
2.7.1 Certifieringar och avtal

Heit har en mängd olika certifieringar. De som vi finner mest intressanta för den här studien är ISO 9001:2008 samt ISO 27001:2005.

När Heit tecknar ett nytt avtal som innefattar överföringar av personuppgifter till tredje land används de standardavtalsklausuler som finns förklarade i personuppgiftsförordningen.

2.7.2 Exempel på teknisk lösning

För att Heit ska kunna säkerhetsställa att avtalen och lagen följs har de en avancerad teknisk lösning som ser till att de berörda individerna i ett tredje land inte kan göra mer än nödvändigt i systemen. Nedan finns en figur som visar deras lösning.



Figur 2.2 (Georgson och Kristiansson)

Steg 1
I det första steget går användaren in på en webbsida och detta kan ske från hela världen. På webbsidan autentisering sig användaren mot en av Heits servrar som hanterar användarinformation (AD). Användarhanteringen är uppbyggd kring roller vilket gör att användare får olika roller som avgör vilken information de har tillgång till. Detta går att styra på detaljnivå och på så sätt minimeras risken att en användare i tredje land får tillgång till data som inte är avsett för behandling i tredje land.

Steg 2
Användaren skickas till ett webbinterface på den virtuella instans som motsvarar den roll som följer vad som angivits vid inloggningen. Steg 2 är alltså en mängd virtuella maskiner som var och en stödjer en användare med en roll, för en miljö, maskin eller kund, beroende på krav. Det kan alltså vara en medarbetare placerad i tredje land som är användare.

Steg 3
I det tredje steget går det bara att jobba med en miljö i taget och ingen data går att flytta mellan de olika miljöerna. En miljö består vanligtvis av en eller flera virtuella maskiner.

Servrarnas fysiska placering är Sverige eller annat land inom EU/EES. Informationen lagras med andra ord aldrig i ett tredje land. Det går inte för en användare i ett tredje land att spara ner eller skriva ut information. Det en användare i tredje land arbetar med kan vara exempelvis korrigering av felaktiga uppgifter eller felsökning i applikationer utifrån serviceärende.

Heit anser att en sådan här lösning medför att ett regelverk kan implementeras på vad användaren har får åtkomst samtidigt som registrering av vilka åtgärder eller uppgifter som personalen access kan registreras. Ett av de enklaste alternativen hade annars varit att skapa ett virtuellt privat nätverk (VPN) där användaren i tredje land får tillgång till hela nätverket där informationen finns lagrad på servrarna. Detta hade inneburit sämre kontroll och de hade helt enkelt inte kunnat garantera att allt går rätt till.

Notera att ovanstående information är en förenkling av sekretessbelagd information och att vi av den anledningen inte kan hänvisa till något källmaterial.

2.8 Debatten i Sverige

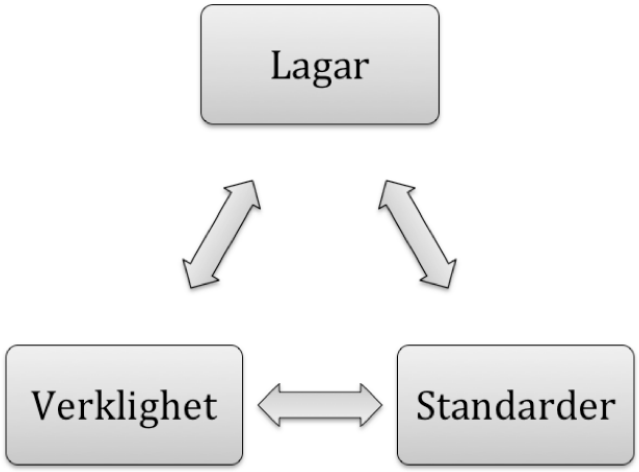
Vi har inte identifierat någon större debatt i Sverige. Det finns tre artiklar som vi anser är av intresse för den här studien. En av dessa handlar om just att det inte finns någon debatt i Sverige (Computer Sweden: debatt, 2013). I artikeln menar den intervjuade personen att det är hög tid att börja debattera förslaget i Sverige.

I en annan artikel i Computer Sweden (Computer Sweden: hemlig lobbying, 2013) menar författaren på att tre stora amerikanska företag jobbar hårt med s.k. lobbyverksamhet för att få förslaget att bli friare. Vilket då leder till en friare behandling av personuppgifter.

Även Svenska Dagbladet (2013) har skrivit om förslaget. De är inne på samma spår som Computer Swedens artikel om lobbying (Computer Sweden: hemlig lobbying, 2013). I artikeln beskrivs hur de stora företagens lobbying är den mest omfattande någonsin samt hur förslaget riskerar att urvattnas. Enligt artikelförfattaren är anledningen till detta att de stora amerikanska företagen tjänar stora pengar på att ha mycket information om personer och därmed lägger stora summor på sin lobbyverksamhet.

2.9 Sammanfattning

Vi har under vår litteraturgenomgång identifierat tre viktiga områden som är centrala i vår studie och att de påverkar varandra. De tre är lagar, standarder och verklighet. Lagarna har vi undersökt genom att studera både nuvarande och kommande lagstiftning. Dessa lagar kan sedan med fördel följas genom användandet av en korrekt och övergripande syn på informationssäkerhet samt med hjälp av standarder och vedertagna metoder. Lagar och standarder ska sedan i sin tur kunna följas och användas i verkligheten. I vårt fall är verkligheten baserad på vårt studieobjekt eftersom vi anser att deras arbetssätt är överförbart på andra organisationer. Samtliga pilar är dubbelriktade då alla delar påverkar varandra. Detta har vi valt att visualisera med följande modell:



Figur 2.3 (Georgson och Kristiansson)

3 Metod

Vi kommer i det här kapitlet beskriva hur vi har gått tillväga för att samla in data som täcker in hela vår modell som vi beskrev i 2.8. Vi anser att vi med vår data har skapat en heltäckande bild av problemområdet, som sedan analyseras i nästa kapitel.

3.1 Val av metod

Enligt Jacobsen (Vad, hur och varför? 2002, s. 34) är en deduktiv strategi när forskningsfrågan behandlas utifrån någon form av förväntningar. Det betyder ofta att det finns förutfattade meningar eller en förväntad bild av slutresultatet innan studien påbörjas. I vårt fall blir det mestadels motsatsen eftersom att vi ger oss in på något som vi inte har haft mycket kontakt med tidigare. Det vi har haft kontakt med innan är informationssäkerheten, men vårt problemområde som innefattar en del juridik är något vi inte har mycket förkunskaper om. Ännu mindre kunskap har vi om förslaget och hur det skulle kunna påverka arbetet med informationssäkerhet. Därför anser vi att vår strategi till största del istället är induktiv, motsatsen till deduktiv.

Eftersom studien berör ett ämne som endast ett begränsat antal personer känner till och förstår så har undersökningsmetoden varit kvalitativ. Dessutom fanns det inget som är mätbart eller hade varit till grund för en kvantitativ undersökning.

3.2 Primärdata

Enligt Jacobsen (2002, s. 152) är primärdata sådana data som samlas in direkt från en person eller som kommer direkt från en organisation. Vår primärdata består av förslaget till förordningen, intervjuer och sammanställningen av Heits arbete kring informationssäkerhet.

Vårt problemområde gjorde att vi först och främst studerade det förslag till förordning som fanns tillgängligt. För att få relevant bakgrundsinformation använde vi oss av de gällande lagar och förordningar som fanns samt DIs förklaringar på sin webbplats. Informationen kom alltså från källor med hög trovärdighet och därmed var behovet av källkritik lågt.

Vår primärdata i den här studien grundar sig även på information som vi sammanställde tillsammans med Heit över deras situation. Då den bygger på sekretessbelagd information har vi ingått ett sekretessavtal med Heit och därför kan delar av datan bara presenteras i förenklad och anonymiserad form. I detta fall kunde vi inte kontrollera att Heit faktiskt jobbar på det sätt som de har informerat oss om utan vi får helt enkelt utgå från att så är fallet.

Vidare har vi genomfört intervjuer med personer som har insikt i ämnet och förståelse för den aktuella problematiken. Dessa personer har även fått förklara en del saker som inte har varit lätt att förstå för oss som inte har den juridiska kunskap som ibland har krävts.

3.3 Sekundärdata

Jacobsen (2002, s. 153) menar på att sekundärdata är data som är insamlad av någon annan. Vilket alltså betyder böcker och artiklar som har skrivits i ett annat syfte. I vårt fall har vår sekundärdata bestått av böcker om informationssäkerhet samt vetenskapliga artiklar inom området. Avsaknaden av debatt kring problemområdet gör att det inte fanns några vetenskapliga artiklar i ämnet och det fanns dessutom ytterst få artiklar av annan karaktär som var av intresse.

3.4 Intervjuteknik

Eftersom våra intervjuobjekt besatt olika sorters kunskap och var tänkta att tillsammans ge en bild av vårt problemområde var våra intervjuer till en viss del standardiserade. Dock har frågorna anpassats beroende på vem som intervjuas och vi har även bett intervjuobjekten att utveckla svaren när det har varit möjligt. Det leder till att vi valde att kalla våra intervjuer semistandardiserade (Lundahl och Skärvad 1999, s. 116).

Vidare kan våra intervjuer ses som både strukturerade och fria på samma gång. Det beror på att vi endast hade begränsad kunskap inom problemområdet och då behövde ha mycket information från kunniga personer, vilket alltså är ett kännetecken för en strukturerad intervju enligt Lundahl och Skärvad (1999, s. 118). De menar vidare att en fri intervju är en intervju där det lämnas utrymme åt personliga tankar och åsikter, vilket vi även gör. Därför kallade vi vår intervjuteknik för “semistandardiserad och fritt strukturerad”.

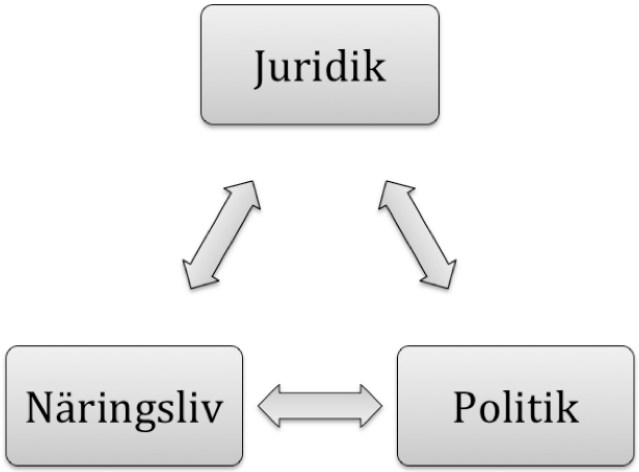
Då vi inte hade någon möjlighet att träffa våra intervjuobjekt fysiskt var det naturligt att utföra intervjuerna via telefon. Dock ville Heit inte låta sig spelas in utan vi hade först en diskussion kring frågorna och sedan skickade de sina svar via e-post. Peter Gerhard träffade vi i verkligheten och genomförde intervjun.

3.5 Intervjuobjekt

När vi letade efter lämpliga intervjuobjekt kom vi snabbt fram till att det inte är många personer i Sverige som är insatta i ämnet. Det var något som något senare styrktes av en artikel i Computer Sweden (2013). Därför valde vi att intervjua Elisabeth Wallin, jurist och internationell samordnare på DI, och Amelia Andersdotter, EU-parlamentariker med särskilt intresse för integritetsfrågor, samt Peter Gerhard som är universitetslektor vid institutionen för handelsrätt på Lunds universitet och en anonym person på Heit vars titel är “Lead Security Officer”.

Genom att vi intervjuade både Gerhard och Wallin fick vi två olika juridiska synvinklar på förslaget. Det ser vi som positivt då det är komplicerat att sätta sig in i vad förslaget får för konsekvenser.

På så sätt skapade vi en figur som består av tre delar. En del består av juridiken, en politisk och till sist näringslivet. Det gjorde att vi bedömde att vi fick en bra fördelning av intervjuobjekt och därmed kunde skapa en relevant bild. Som vi ser det påverkar dessa tre varandra likt vår tidigare triangel och alla parter berördes av varandra som vi visualiserar på följande sätt:



Figur 3.1 (Georgson och Kristiansson)

Denna modell kan kopplas ihop med vår modell i 2.8 eftersom att det finns en likhet i att juridiken och politiken ska skapa en verklighet som näringslivet befinner sig i. Det skapas med andra ord en form av verklighet som organisationerna befinner sig i. Likt den tidigare modellen påverkar även alla delar i den här modellen varandra, därav de dubbelriktade pilarna.

Vi försökte även komma i kontakt med en rad andra personer men en del svarade inte och en svarade att han inte själv ansåg sig tillräckligt kunnig inom området. Det ledde till att vår empiridel blev något mindre än vi först önskade. Det är möjligt att det finns många personer utanför Sverige som är väl insatta i det här ämnet. Vi har dock valt att begränsa oss till personer inom Sverige eftersom att vi anser att det är viktigt att förstå skillnaden mellan bl.a. PUL och den nya förordningen.

3.6 Intervjuguide

Då problemområdet för den här studien var ett förslag till en förordning, som det har varit komplicerat att sätta sig in i, har intervjuerna utformats på ett sådant sätt att de ska ge mer information om detta. Samtliga frågor finns i bilaga 1: intervjufrågor. Vi har delat in våra intervjuer i tre delar.

3.6.1 Första delen

I första delen var vi intresserade av att få veta hur respondenterna ser på behovet av en ny förordning och om denna i så fall överensstämmer med EU-kommissionens motivering som vi skrev om i 2.5.1. Dessutom vill vi få svar på huruvida artikeln i Computer Sweden

(Computer Sweden: debatt, 2013) hade rätt i det påstående de gör om att Sverige är ett av få länder som vill ha det här förslaget som ett direktiv istället för en förordning. I de fall respondenterna är väl insatta i den frågeställningen ställde vi följdfrågor.

3.6.2 Andra delen

I andra delen gick vi in på respektive respondents organisation eller närområde för att undersöka hur de kommer påverkas. För att ta reda på vad IT-företagen kan förvänta sig för hjälp ställde vi i intervjun med Elisabeth Wallin frågan om hur DI kan komma att agera gentemot företagen. Det gjorde vi eftersom vi har förstått att det var oklart och att det inte är helt okomplicerat att ta till sig en lagförändring.

I intervjun med Amelia Andersdotter undrade vi hur Piratpartiet kommer gå tillväga eftersom vi är nyfikna på hur partiet kommer agera för att försöka skapa en debatt i media. Vi ville också veta hur arbetet med förslaget kommer fortlöpa inom EU-kommissionen och EU-parlamentet. Detta eftersom att vi inte lyckades identifiera någon större debatt trots att det är ett ämne som berör hela samhället på längre sikt.

I intervjun med Heit fokuserade vi på hur de arbetar idag med informationssäkerhet, hur de tror att konkurrenterna arbetar samt hur och var förordningen diskuteras i organisationen. Samt deras allmänna syn på informationssäkerhet för att kunna se om de jobbar på ett sätt som överensstämmer med de metoder vi har identifierade under 2.2 och 2.3 i vår litteraturgenomgång.

3.6.3 Tredje delen

Den sista delen hade fokus på detaljfrågor som vi kände att vi inte har kunnat få klarhet i genom vår litteraturgenomgång. Här var vi exempelvis intresserade av att se hur våra respondenter såg på standardavtalsklausuler och BCR för att undersöka om det stämde överens med vår bild. Vi har även i 2.5.10 skrivit om påföljderna vilket vi hade svårt för att bedöma om de ligger på en rimlig nivå eller inte och därför ställer vi en fråga om det till samtliga respondenter. Intervjun avslutas med frågan “Har du något annat att tillägga gällande ämnet?“ i samtliga fall för att se om våra respondenter hade något mer att berätta.

3.7 Etik

Vi har i vår studie gjort etiska övervägande vid en rad olika tillfällen. Företaget som har varit studieobjekt har valt att vara anonyma vilket vi respekterade. Vidare var vi noga med att förklara för våra intervjuobjekt om vilka vi är och vilket syfte vi hade. Intervjuobjekten har även blivit informerade om att de fick vara anonyma om de ville och har lämnat sitt samtycke till att vi spelade in intervjuerna.

3.8 Validitet och reliabilitet

När vi genomförde undersökningen hade vi begreppen validitet och reliabilitet i åtanke. Det för att det ska finnas en riktlinje för hur kritiskt man ska agera gentemot de datakällor som har använts. Det går till som så att man går efter tre frågor (Jacobsen 2002, s. 20-22): Har vi fått tag i vad vi ville ha (intern validitet)? Kan vi överföra det som vi funnit till andra sammanhang (extern validitet)? Kan vi lita på de data vi samlat in (reliabilitet)?

Validiteten utgår ifrån att empirin är giltig och relevant. Eftersom vi har fått tag i intervjuobjekt vars spetskompetens är just det området som vi undersöker anser vi att validiteten är på en hög nivå. Sen så har vi kommit över källor som har verkat aktuella.

Vårt ämne är av en generell karaktär då det är något som kommer beröra de flesta stora IT-bolagen i hela EU. Dessa kommer med andra ord kunna ta till sig av undersökningen för att kunna vara förberedd på det nya lagförslaget.

Reliabilitet utgår från att empirin är trovärdig, med andra ord att faktan som vi har fått från våra olika källor är korrekta. Det utgår vi ifrån delvis på samma sätt som vi utgår från dess giltighet. Eftersom ett av våra intervjuobjekt representerar ett politiskt parti, vars åsikter speglar dennes ideologiska uppfattning om förslaget, har den här intervjun hanterats mer källkritiskt än övrigt material. En annan sak som också måste tas i åtanke är att förslaget fortfarande är under utveckling vilket innebär för vår studie att ingen kan ge ett helt klart besked om hur det slutgiltiga förslaget kommer att se ut. Då det finns få personer är tillräckligt insatta ämnet för att kunna besvara frågeställningen har ändå intervjuer genomförts med experter och intressenter på området så ser vi det som att reliabiliteten generellt sett är av hög nivå.

Frågeställningen är kvalitativ eftersom ämnet är sådant att relativt få personer besitter någon kunskap inom det. Därför har stor vikt lagts vid att ta se till så att intervjuobjekten är sådana som bidragit med information som är relevant och trovärdig för forskningen och frågeställningen (Jacobsen 2002, s 56-57).

Studieobjektet har studerats utifrån den nivån att vi har fått insyn hur man precis som sina främsta konkurrenter. Därmed så är resultatet vi fått fram tillämpbart även på andra aktörer vilket innebär att resultatet kan ses som generellt.

Studieobjektets arbetssätt har studerats utifrån en övergripande nivå där vi inte har gått ner och tittat på tekniska detaljer. Utifrån det här perspektivet har vi gjort ett antagande om att det här arbetssättet är generellt beskrivet på ett sådant sätt att det är överförbart till liknande företag. På så sätt anser vi att vi når hög extern validitet (Jacobsen 2002, s. 21).

4 Empiri

Vi kommer i det här avsnittet sammanfatta det vi fick fram från våra fyra intervjuer. Fullständiga svar finns i bilagorna.

4.1 Nya dataskyddsförordningen

Det råder ingen tvekan om att det behövs en ny dataskyddsförordning då den nuvarande lagstiftningen anses föråldrad eftersom tekniken har förändrats i hög takt som vi skrev om i 1.1. Vidare är det välkommet med ett starkare skydd för den enskilde individen. Det är också positivt att EUs medlemsstater får en mer enhetlig lagstiftning. Elisabeth Wallin uttrycker det så här:

> ”Att förstärka den registrerades rättigheter är ju något som vi stödjer. Och det är klart att det är bättre om man kan ha en mer likartad reglering över hela EU eftersom människor rör sig mellan länderna och så.”

Medan Amelia Andersdotter ser på det så här:

> ”Ja, vi behöver uppdatera personuppgiftslagstiftningen. Den är inte alls tidsenlig och den har inte haft dom effekter vi vill att dataskyddslagstiftningen skulle ha i Europa så att det har funnits ett behov av en reform har varit ganska uppenbart under väldigt många år redan men det är ett ganska stort område att reformera och därför har det dröjt med att ta fram ett förslag för det krävs mycket politiskt mod att lägga ett sånt förslag”

Även Heit uttrycker sig positivt om förslaget:

> ”Vi får bättre kontroll på hur vi hanterar denna typ av information och gemensamma regler EU. Förslaget är bra. Det ger en större förståelse för problematiken kring behandling av personuppgift.”

Peter Gerhard är även han generellt sett positiv till att det kommer en ny förordning, även om han är skeptisk till vissa bitar som vi återkommer till senare.

4.2 Debatten i Sverige

Något vi har uppmärksammat i 2.8 är att det inte förs någon större debatt i Sverige, vilket även stärktes av en artikel i Computer Sweden (Computer Sweden: debatt, 2013). När vi frågade Heit om detta svarade de:

> ”Individen själv begriper inte vad som kan göras med den information som är samlad. Problemet att ingen förstår konsekvenser av behandlingen och hur detta påverkar mig

> som medborgare. Oftast hänvisas till det förhärskande ’rent-mjöl-i-påsen’-uppfattningen, vilken är en skymf emot den mänskliga rättigheten till ett privatliv.”

Även Gerhard är inne på att individerna inte förstår förslaget då det är svårt att sätta sig in i det och även för att det har en tendens till att vara tekniskt komplicerat. Vilket han dock är något förvånad över då det handlar om individers skydd.

4.3 Direktiv eller förordning

Enligt en artikel i Computer Sweden (Computer Sweden: debatt, 2013), som vi skrev om i 2.8, är Sverige ett av de få länder som vill ha förordningen till ett direktiv istället. Detta hade inneburit att länderna hade kunnat agera friare och stifta egna lagar. Enligt Andersdotter kommer det inte bli något direktiv av det hela, det är ingenting som diskuteras. Wallin ser fördelar med båda alternativen och menar på att olika länder har olika förutsättningar och lagar men att om det blir ett direktiv missas nog målet med ökad harmonisering. Det kan dock bli problematiskt med en förordning där det inte tas hänsyn till de olika förutsättningarna.

Enligt Gerhard finns generellt sett en vilja inom Sverige att EU bör fokusera på direktiv istället för förordningar. Detta grundar sig i följande:

> “Vi var först i världen med en datalag, tror jag, när den kom. Så vi tycker att vi ligger långt fram. Så det räcker för oss att ha ett mål så kan vi själva se till att det uppnås medan alla andra länder, ja, dom kan väl tycka att en förordning med detaljstyrning är enklare så slipper dom hitta på så mycket själva, då kommer alltihop färdigt.”

Vidare menar Gerhard att det kanske inte spelar så stor roll i sig om det blir en förordning eller direktiv då det i slutändan är hur det tillämpas i olika länder som faktiskt spelar någon roll. Här ser han en risk i att det kan tolkas på olika sätt i olika länder som har olika kulturer och traditioner.

4.4 Datainspektionen

Som vi nämnde i 2.4.2 och 2.5.7 ska varje land ha en tillsynsmyndighet för att kontrollera att förordningen följs. I Sverige är det Datainspektionen (DI) som även fortsättningsvis kommer att vara tillsynsmyndighet. Wallin tror inte att förordningen kommer förändra DI som organisation nämnvärt:

> ”Vi som organisation tror jag inte kommer påverkas så mycket, rent storleksmässigt eller så. Eller vad vi har för befogenheter, det kommer nog i stort sett vara samma. Däremot är ju en tanke med förordningen att dataskyddsmyndigheterna i EU-länderna ska samarbeta mycket mer.”

Vi har under studiens gång konstaterat att det inte alltid är helt lätt att sätta sig in i förordningen och vi undrade därför vad olika organisationer kan förvänta sig att få för hjälp från DI. Enligt Wallin kan företagen inte förvänta sig mycket mer än allmän information och vägledning.

4.5 Standardavtalsklausulernas framtid

Vi har förstått att standardavtalsklausulerna som vi gick igenom i 2.4.5 är en kritisk fråga för vår uppdragsgivare. En förändring av reglerna kring dem skulle kunna få stora konsekvenser men det verkar inte vara aktuellt enligt Wallin. Hon säger att det finns stöd för standardavtalsklausuler även i förslaget. I artikel 42 nämns det under benämningen apporiate safe guards. Hon tror även att utgångspunkten har varit att de standardavtalsklausuler som används idag även i fortsättningen ska vara giltiga och användas.

När Gerhard fick höra att Wallin utgår från att standardavtalsklausulerna blev han förvånad och menar på att det är rimligt att även dessa görs om för att säkerställa att skyddet för individerna stärks. Han tror inte att de är så välutvecklade och välutformade att de kan användas även i fortsättningen.

4.6 Förenklade BCR

En annan bestämmelse som kan komma att påverka vårt studieobjekt är Binding Corporate Rules (BCR). Den nuvarande situationen gick vi igenom i 2.4.4. Både Andersdotter och Wallin menade på att dessa i fortsättningen kommer vara mer användbara men att de bara får användas inom koncerner. Detta innebär alltså att en organisation som anlitar ett IT-företag kan känna sig trygga med att deras information inte hamnar i ett annat land p.g.a. BCR.

När vi frågade Heit om hur de ser på BCR menade de på att idén är god, men att det idag inte tillför tillräckligt värde i förhållande till de resurser som krävs vid införandet.

4.7 Synen på adekvat skyddsnivå

Enligt Wallin har DI i sitt remissvar till regeringen haft synpunkter på bedömningen av adekvat skyddsnivå:

> ”Då tyckte vi, tolkade vi dom här bestämmelserna om tredjelandsöverföringar som att man inte längre själv kan göra nån bedömning om det finns en adekvat skyddsnivå eller inte. Som personuppgiftslagen och direktivet är formulerat idag så finns det ett stycke som säger vilka omständigheter man ska ta hänsyn till innan man gör en bedömning om ett land har adekvat skyddsnivå eller inte. Då har vi tolkat det som att i princip kan man göra den bedömningen själv, sen har ju kommissionen då när det gäller vissa länder fattat beslut om att de har en adekvat skyddsnivå och då är det ju

> klart och tydligt. Men det har inte funnits något som har hindrat att man har gjort den bedömningen själv.”

Wallin påpekar dock även att sådana bedömningar är väldigt svåra att göra. Gerhard menar att just begreppet adekvat skyddsnivå är oklart och att det därmed inte är ett bra begrepp att ha med i förordningen.

4.8 Hantering av personuppgifter

Andersdotter anser att företag skulle kunna se annorlunda på hanteringen av personuppgifter:

> ”Vi behöver alltså reglera den här sektorn på ett sådant sätt att det bästa ett företag kan göra är att vara mer privatlivssäkert än ett annat företag istället för tvärtom så att man får konkurrensfördelar av att ta tillvara på medborgarnas självbestämmande anonymitet och det är ju sånt som politiker kan göra om dom vill.”

Andersdotter är även oroad över hur personuppgifterna hanteras och hur tillgängligheten från tredje land hanteras:

> ”...ett lite mer enkelt fall, kan man komma åt det från Indien, ja då kan man ju komma åt det från Turkiet också och är man till exempel en svensk kurd då kanske man inte vill att turkarna ska sitta och komma åt ens medicinska journaler på håll.”

4.9 Påföljder

Ytterligare en sak som ändras i förordningen är påföljderna vid en överträdelse och i 2.5.10 konstaterade vi att de blir hårdare än idag. När vi tar upp detta med våra respondenter går meningarna isär. Wallin anser att det är möjligt att bötesnivåerna är rimliga, men att det borde vara upp till tillsynsmyndigheterna att bedöma när böter ska utdömas. Andersdotter tycker däremot att bötesbeloppen är orimligt låga och gör en jämförelse:

> ”Och då kan man egentligen säga att det är ju inte så mycket pengar bara 2% av omsättningen. Vilket är sex gånger så lite som man betalar till exempel för konkurrensöverträdelser, så även där har ju egentligen kommissionen varit väldigt väldigt försiktig kan man säga. Det borde egentligen vara hårdare sanktioner mot företag som beter sig dumt.”

Även Gerhard är inne på samma spår:

> “Jämför du med konkurrenslagen så ligger den på 10 % och då kan det vara hela koncernens omsättning. Så det kan bli våldsamma belopp men det döms ju aldrig ut men 2 % verkar lite mesigt. Varför drar man inte en parallell till konkurrenslagen då? Som ju också är internationell på det viset.”

Heit menar på att de anser att påföljderna är rimliga och anser att det är viktigt för branschen att bötesbeloppen blir kännbara, men samtidigt måste det gå att göra ett misstag. Det innebär att de tycker att det inte får finnas en risk för att en bot resulterar i att företag går i konkurs.

4.10 EU och USA

Andersdotter riktar även kritik mot EUs samarbete med USA. Hon menar på att EU är väldigt välvilligt inställda till USA trots att kommissionen inte har beslutat att USA har en adekvat skyddsnivå. Enligt henne överförs personuppgifter relativt fritt från EU till USA. Detta ser hon som riskfyllt då USA generellt sett ser personuppgiftsskydd som en konsumenträttighet istället för en mänsklig rättighet som det är inom EU.

4.11 Förslagets framtida utveckling

Våra respondenter hade svårt att gissa hur det slutgiltiga förslaget kan komma att se ut då de var överens om det finns många krafter som försöker påverka det, något vi skrev om i 2.8. Både Andersdotter och Gerhard menar på att det finns en överhängande risk för att förslaget blir uttunnat och att ytterligare undantag förs in.

4.12 Informationssäkerhet och kvalitetssäkring

I 2.2 skrev vi om olika sätt att skydda information på inom ett företag och var därför intresserade av att höra vad Heit hade att säga om detta. De anser att policys är ett grundläggande skydd som måste finnas inom ett företag. Det är också viktigt att det inte blir för många olika policys samtidigt som en policy måste vara väl förankrad i verkligheten och fungera som det är tänkt.

De anser även att kvalitetssäkringen är en väldigt viktig bit och menar på att det är svårt att få några kunder utan dessa standarder. Dessutom påpekar de att de jobbar på ungefär samma sätt som deras konkurrenter:

> “Ja, det finns inte så många andra möjligheter att hantera detta på om man är medveten om problematiken. Det ökar förståelsen mellan kund och leverantör. Det är mer eller mindre ett krav från våra kunder att vi har ISO 27000 och ’kör’ enligt ITIL.”

4.13 Sammanfattning

För att sammanfatta våra respondenters svar och åsikter presenterar vi här nedan en tabell över de fem viktigaste frågorna. I några fall har inte samma fråga diskuterats med alla respondenter och benämns då med “Frågan ej diskuterad”.

	Wallin	**Andersdotter**	**Gerhard**	**Heit**
Allmän uppfattning	Positiv till att individens skydd stärks.	Tycker att det är hög tid att modernisera lagstiftningen.	Positiv till att EU vill stärka individens rättigheter men skeptisk till att det faktisk blir någon större skillnad.	Bra att det blir en enhetlig lagstiftning inom hela EU. Förenklar deras jobb med överföringar.
Varför finns det ingen debatt?	Frågan ej diskuterad.	Kommer jobba för att få igång en debatt som är sanningsenlig m.h.a. debattartiklar m.m.	Tror att den är för tekniskt komplicerad men ändå förvånad över att det är så tyst.	Tror inte individerna förstår konsekvenserna av förslaget.
Förordning kontra direktiv	Blir det en förordning och inte ett direktiv blir det komplicerat med vissa speciallagar som finns i Sverige.	Det är inte aktuellt. Inom EU förs det ingen sådan debatt.	Sverige har ett väl fungerande rättssystem och har länge legat i framkant med datalagar och därmed anser vi oss inte ha ett behov av en fyrkantig förordning.	Frågan ej diskuterad.
Vad tror du om förslagets framtid?	Kommer nog förändras en del. Mycket debatt inom EU just nu.	Det kommer att urvattnas. Första förslaget var bra men det är väldigt mycket lobbyorganisationer som jobbar med det här.	Förmodligen kommer det att komma fler undantag och därmed urvattnas ännu mer. Det är en komplicerad förordning.	Frågan ej diskuterad.
Är påföljderna rimliga?	Det är möjligt men däremot borde Datainspektionen själva få avgöra när det ska utdömas böter.	Nej, de är alldeles för låga. Se på konkurrenslagstiftningen, de ligger på en mer rimlig nivå.	Ifrågasätter varför man inte drar en parallell till konkurrenslagstiftningen. Även om det sällan döms ut maxbelopp så är det bra att det är högt satt.	Ja, det är rimligt. Det är tillräckligt högt för att det ska kännas samtidigt som det inte riskerar att få ett företag att gå i konkurs.

5 Analys och diskussion

I den här delen kommer vi analysera och tolka det som vi har gått igenom i vår empiri och knyta samma detta med det vi fick fram i vår litteraturstudie.

Det som är viktigt att komma ihåg är att vi i den här studien bara har fokuserat på de delar som rör överföringar till tredje land. I media har det bland annat rapporterats om andra skillnader som kan få betydligt större konsekvenser. Det är bland annat att den registrerade ska ha rätt att bli borttagen och även föras över till andra system (Comupter Sweden: debatt 2013).

5.1 Förändringar

Vi konstaterar med stöd av vår egen tolkning av förslaget samt Elisabeth Wallins uttalande (se 4.4, 4.5 och 4.6) att det inte kommer att bli några dramatiska förändringar för svenska företag som förslaget ser ut just nu. Nästa sak som vi kan konstatera är att det finns goda skäl till att tro att det kan komma in en hel del förändringar till den förordning som kommer att träda i kraft, vilket inte minst stöds av de artiklar som vi skrev om i 2.8. Vår uppfattning är att det senare i år kommer vara tydligare hur det slutgiltiga förslaget kommer att se ut.

Det som vi ser som den största förändringen är påföljderna som skrev om i 2.5.10. Det innebär att vid en överträdelse kommer bötesbeloppen vara betydligt mer kännbara än tidigare. Det har dock visat sig att det finns personer, som exempelvis Andersdotter, inom EU-parlamentet som vill ha ännu högre bötesbelopp (se 4.9). Vilket leder till att företagen bör bli mer måna om att följa förordningen.

Det som vi ser som ett positivt tecken för vårt studieobjekt är att Wallin menar att EU-kommissionen har utgått från att de standardavtalsklausuler (se 2.4.5) som finns idag även ska gälla i fortsättningen (se 4.5). Det gör att det finns anledning till att tro att en lagförändring i praktiken kan gå ganska obemärkt förbi i de fall där parterna har slutit ett avtal med stöd av standardavtalsklauserna.

Vi ser även det som positivt att EU-kommissionen vill förändra reglerna kring BCR (se 2.5.5). Exakt hur det kommer förändras är något oklart. En sak som vi ser som en klar förbättring är att en BCR i framtiden inte behöver godkännas av en tillsynsmyndighet för att vara giltig. Wallin menar också på att det är positivt att begreppet BCR numera finns med i en förordning och på så sätt har blivit ett vedertaget begrepp (se 4.6). Om förordningen lyckas göra BCR enklare och mer användbart kan det mycket väl visa sig vara intressant för det undersökta företaget, vilket de inte tycker idag (se 4.6). Viktigt att komma ihåg här är att detta bara gäller för överföringar inom koncerner och inte av så kallad kunddata.

Trots avsaknaden av debatt i Sverige, som vi skrev om i 2.8, kan vi konstatera att alla som vi har kommit i kontakt med under vår studie är positivt inställda till att det kommer en förordning (se 4.1). Främst för att denna kommer att öka skyddet för de registrerade och för att det blir ett tydligare regelverk för samtliga EUs medlemsstater. Vi har även märkt att debatten har kommit igång något i slutet av våren men ingen av de artiklar vi har kommit i kontakt med har nämnt tredjelandsöverföringar.

5.2 Tillämpning

En viktig del av förordningen som det inte skrivs eller talas särskilt mycket om är de skyddsåtgärder som företag måste vidta för att upprätthålla en tillräckligt hög säkerhetsnivå. Det är därmed oklart hur företagen bör förhålla sig till detta. Vi valde därför att studera olika metoder, standarder och lösningar för att hantera sin information säkert.

5.2.1 Vår syn på informationssäkerhet

Vi kan genom vår litteraturstudie konstatera att informationssäkerhet i grund och botten inte är ett tekniskt problem som ska läggas på ett företags IT-avdelning att lösa (se 2.2.1). Det är viktigt att företag arbetar med informationssäkerhet på alla nivåer inom organisationen. Som vi ser det är det viktigt att såväl ledningen som alla anställda är medvetna om hur betydande säkerheten är och att de rutiner som finns faktiskt efterföljs.

Vidare är det viktigt att förstå vad en attack, en borttappad enhet eller ett haveri kan få för konsekvenser. Samtidigt som företag som jobbar med olika former av system måste sträva efter att göra säkra lösningar måste de även vara användarvänliga (se 2.2.1). Eftersom Bunker (2011, s. 24) menar på att det dessutom är vanligt att företag inte vet var deras information lagras gör vi bedömningen att både vårt studieobjekt, och andra företag i branschen, samt deras kunder måste bli bättre på att förstå och förmedla detta. Det blir givetvis extra viktigt när vi som i det här fallet diskuterar överföringar till ett tredje land.

För att få en bra överblick av arbetet med informationssäkerhet i en organisation anser vi att en modell kan vara en bra utgångspunkt. I 2.2.2 skrev vi om CIA-triangeln och vi tycker att det kan vara relevant att kolla på den. Det anser vi eftersom den tar med viktiga delar som lagen indirekt kräver. Vi tänker framför allt på integritetsdelen som i denna studie är oerhört viktig. Det är den del vi bedömer att företag som jobbar med överföring till tredje land måste lägga mest vikt vid. Brister denna del är risken för att information hamnar i orätta händer överhängande vilket i sin tur kan leda till böter (se 2.5.10).

Till sist är det även viktigt för företag att komma ihåg den mänskliga faktorn (se 2.2.5). Den går aldrig att bortse från och finns alltid med som ett orosmoln. Människor begår ofta misstag och konsekvenserna kan bli mycket stora. Det kan röra sig om allt från att en anställd på ett företag tappar bort en enhet eller öppnar en webbsida med elak kod. Det gör att företagen måste bygga säkra interna system och på så sätt minska konsekvenserna av mänskliga misstag.

5.2.2 Olika former av skydd

Det finns idag en mängd olika tekniska lösningar för att skydda sin information. Då studien främst fokuserar på IT-företag förutsätter vi att de besitter den kunskap som behövs. Det vi istället har valt att fokusera på är vad det finns för olika best practise-lösningar samt hur organisationer kan begränsa sina anställda genom att använda sig av olika kontrollsystem (se 2.2).

Först och främst anser vi att ett företag måste ha en rad olika policys (se 2.2.3) som förbinder de anställda att arbeta på ett visst sätt, vilket även det undersökta företaget håller med om (se 4.12). För att de anställda ska kunna ta till sig en policy är det viktigt att den är korrekt utformad och enkel att förstå samt att den ständigt hålls aktuell. Det är som sagt även viktigt med kontroller av vad de anställda gör (se 2.2.4). En person som blir kontrollerad känner ett större ansvar vilket leder till att han eller hon följer regler bättre. Vi kan även konstatera att det kan vara rimligt att se till så att en person inte kan göra betydande förändringar eller affärskritiska moment helt på egen hand, utan att en annan person måste godkänna innan allt tas i bruk (se 2.2.3).

Vi har även uppmärksammat att det är rimligt att ställa krav på de system som finns när det kommer till spårbarhet (se 2.2.4). Det är viktigt att det går att se vem som har gjort vad. Det tror vi kan vara helt avgörande om ett företag hamnar i en situation där det anklagas för ha gjort ett lagbrott. Finns det då mycket bra information om vem som har gjort vad i systemet bör det göra det enklare för dataskyddsmyndigheten att avgöra var det har brustit och därmed kunna utdöma korrekt bötesbelopp, om de finner anklagelserna korrekta.

5.2.3 Säkerhet och kvalitet

Vi anser att när en kund ska lägga ut personuppgifter hos ett IT-företag bör kunden ställa höga krav på att de kan garantera en mycket hög skyddsnivå. Att kontrollera det kan förstås vara mycket svårt men det finns vissa saker som gör det lättare. Vi har i 2.3 identifierat främst två stycken ISO-standarder som vi finner det rimligt att ett IT-företag följer. Dessa är ISO 9001 och ISO 27001. Genom ISO 9001 kan kunden känna sig trygg med att det finns en hög kvalitetsnivå hos IT-företaget och att den kvalitén genomsyrar hela företaget.

Har IT-företaget dessutom en ISO 27001-certifiering (se 2.3.2) säkerställer det att de har en bra nivå på hanterandet av känslig information. Det är förstås extra viktigt när det kommer till personuppgifter och överföringar till tredje land.

Vi kan även konstatera i 2.7.1 att vårt studieobjekt i nuläget använder sig av dessa två certifieringar. Vilket innebär att de står bra förberedda inför en lagförändring som innebär en högre skyddsnivå och ett utökat kvalitetsarbete.

6 Slutsats

Vi ställde oss i början av studien frågan:
Hur kommer ett personuppgiftsbiträde (eller registerförare som det kallas i förslaget) att behöva anpassa sina offshoreåtaganden om EU-kommissionens förslag till ny dataskyddsförordning träder i kraft i sin nuvarande form?

Vårt korta svar på frågan är att om ett personuppgiftsbiträde ser till att skydda sin information på ett bra sätt och försäkrar sig om att kvalitén är hög kommer förslaget inte innebära några dramatiska förändringar. Det är först när det brister och det blir aktuellt med påföljder som den största skillnaden märks, nämligen den nya straffskalan. Vi har även konstaterat att det kan bli mycket enklare att införa BCR, något som borde gynna borde personuppgiftsbiträden och andra koncerner.

Det är dock viktigt att komma ihåg att det här är ett förslag. Vi har i studien försökt blicka framåt för att kunna se vart förordningen kommer att sluta. Det resulterar bara i spekulationer och vi tycker att det är för tidigt att gissa på något. Enligt Andersdotter samt media arbetar stora företag med lobbying vilket givetvis kan påverka förslaget på en mängd olika sätt. Genom att följa medias rapportering framöver kan det vara möjligt att hålla sig uppdaterad om hur det kommer att sluta.

Vi tror att en organisation som använder sig av de metoder och modeller som vi har beskrivit i den här studien står mycket väl förberett inför en ny förordning. Som kund anser vi att det är viktigt att högra krav ställs och att det finns kontroller samt en övergripande förståelse. Att inte veta var ens information lagras ser vi som mycket allvarligt, det är något som ställer krav på både kunden och IT-företaget.

Vidare anser vi inte att det här ämnet lämpar sig för någon vidare forskning så länge det är ett förslag. Däremot hade det varit intressant att se en studie ett par år efter att förordningen har trätt i kraft för att se hur mycket det faktiskt har förändrat företagen och deras arbetssätt.

Personligen hoppas vi även på att debatten i Sverige snart tar fart eftersom vi anser att det här är en fråga som berör individens integritet. Därmed borde det ligga i oerhört många personers intresse att se till att den här förordningen håller en hög nivå. Utgångspunkten för förordningen har trots allt varit att stärka integriteten och om inte de registrerade inte trycker på den punkten är det inte omöjligt att väldigt mycket går lobbyisternas väg.

Källor

Tryckta Källor

Andress, J. (2011). The Basics of Information Security. Waltham: Syngress Media.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. Information security technical report. vol 17. ss. 19-25.

Gillies, A. (2011) "Improving the quality of information security management systems with ISO 27000", The TQM Journal, Vol. 23 Iss: 4, ss.367 - 376

Halvorsen, K. (1992). Samhällsvetenskaplig metod. Lund: Studentlitteratur

Hart, S (2010). Best practices for security and controls for corporate treasurers. Journal of Corporate Treasury Management. Vol. 3 Issue 4. ss. 353-357.

Jacobsen D.I. (2002). Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Lund: Studentlitteratur.

Lundahl, U & Skärvad, P-H. (1999). Utredningsmetodik för samhällsvetare och ekonomer. Lund: Studentlitteratur.

Petlier, T (2005). Information Security Fundamentals. Auerbach Publications

Thompson, H. (2013). The Human Element of Information Security. IEEE SECURITY & PRIVACY; JAN-FEB. Vol 11. ss. 32-35

Elektroniska källor

DI: tredje land. (u.å). Hämtad 2013-05-20
http://www.datainspektionen.se/tredjeland

DI: Personuppgiftslagen. (u.å). Hämtad 2013-04-16. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/)

DI: standardavtalsklausuler. (u.å). Hämtad 2013-04-16.
http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-standardavtalsklausuler/

DI: adekvat skyddsnivå. (u.å). Hämtad 2013-04-16.

http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-menas-med-adekvat-skyddsniva/

DI: binding corporate rules. (u.å). Hämtad 2013-04-16, http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-binding-corporate-rules/

DNVBA: Vad är ISO 27001. (u.å). Hämtad 2013-05-27. http://www.dnvba.com/se/Certifiering/Ledningssystem/Informationssakerhet/Pages/ISO-27001.aspx

EU: Dataskyddsdirektivet. (u.å). Hämtad 2013-04-16. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:sv:HTML

EU: Fördningar och direktiv. (u.å). Hämtad 2013-05-04. http://europa.eu/about-eu/basic-information/decision-making/legal-acts/index_sv.htm

EU: standaravtalsklausuler). (u.å). Hämtad 2013-04-16 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:SV:PDF

"EUs nya datalag måste debatteras i Sverige" (2013). Elektronisk. Computer Sweden, 25 april 2013. Tillgänglig: http://www.idg.se/2.1085/1.504404/eus-nya-datalag-maste-debatteras-i-sverige. Hämtad: 2013-04-25

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning). COM(2012) 11 Final 2012/0011 (COD). Hämtad 2013-04-16 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:SV:PDF

Handfield, R. (2006). A Brief History of Outsourcing. [Elektronisk]. Tillgänglig: http://scm.ncsu.edu/scm-articles/article/a-brief-history-of-outsourcing [2013-05-05]

HP - binding corporate rules. (u.å). Hämtad 2013-04-16. http://www8.hp.com/se/sv/binding-corporate-rules.html

ISO Central Secretariat (2012). Quality management principles. [Elektronisk]. Tillgänglig: http://www.iso.org/iso/qmp_2012.pdf [2013-05-04]

“It-jättarnas hemliga lobbying avslöjad” (2013). Elektronisk. Computer Sweden, 21 maj 2013. Tillgänglig: http://www.idg.se/2.1085/1.508231/it-jattarnas-hemliga-lobbying-avslojad Hämtad: 2013-05-21

SFS (1998:204). Personuppgiftslag. Stockholm: Justitiedepartementet. Hämtad från http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/?bet=1998:204

SFS (1998:1191). Personuppgiftsförordning. Stockholm: Justitiedepartementet. Hämtad från http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftsforordning-1998_sfs-1998-1191/?bet=1998:1191

"Vem ska äga makten över dig på nätet?" (2013). Elektronisk. Svenska Dagbladet, 27 april 2013. Tillgänglig: http://www.svd.se/nyheter/utrikes/vem-ska-aga-makten-over-dig-pa-natet_8211028.svd Hämtad: 2013-04-27

Bilaga 1: Intervjufrågor

Frågor till Elisabeth Wallin, jurist på Datainspektionen:

1. Vad är din generella uppfattning om förslagen? Vad hoppas man vinna, hur påverkar det Sverige och hur påverkar det andra EU-länder?
2. Enligt en artikel i Computer Sweden är Sverige ett av få länder som vill ha detta till ett direktiv istället för en förordning. Är detta korrekt? Varför?
3. Hur bedömer du variationerna i ländernas lagstiftning om det inte blir en förordning?
4. Hur kommer Datainspektionen att påverkas av förslaget?
5. Kommer DI att stödja företagen med tillämpningsföreskrifter eller rekommendationer? Varför väljer DI att göra så?
6. Som vi har förstått det är det i dag vanligt att företag använder sig av standardavtalsklausulerna som finns för överföring av personuppgifter till tredje land. Det nämns inte mycket om dessa i förslaget, kan du berätta mer om hur dessa kan komma att påverkas?
7. Vi tycker att det är otydligt hur Binding corporate rules (BCR) fungerar idag. Kan exempelvis ett IT-konsultföretag som har verksamheter i flera länder sluta ett avtal med en kund som hanterar svenska personuppgifter och sedan fritt överföra dessa uppgifter inom de länderna där koncernen har godkända BCR?
8. Hur har du tolkat att BCR kommer att påverkas av förslaget?
9. Har du noterat andra saker i förslaget som kan komma att påverka överföringar av personuppgifter till ett tredje land?
10. Tror du att det är sannolikt att förslagen kommer att förändras i någon större utsträckning innan de antas? På vilket sätt?
11. Anser du att påföljderna är rimliga? Om inte, vänligen utveckla.
12. Har du något annat att tillägga gällande ämnet?

Frågor till Amelia Andersdotter, EU-parlamentariker, Piratpartiet:

1. Vad är din generella uppfattning om förslagen? Vad hoppas man vinna, hur påverkar det Sverige och hur påverkar det andra EU-länder?
2. Enligt en artikel i Computer Sweden är Sverige ett av få länder som vill ha detta till ett direktiv istället för en förordning. Är detta korrekt? Varför?
3. Hur bedömer du variationerna i ländernas lagstiftning om det inte blir en förordning?
4. Hur kommer Piratpartiet att jobba med förslaget fram till att det kan träda i kraft?
5. Kommer Piratpartiet att försöka skapa en debatt om förslaget?
6. Som vi har förstått det är det i dag vanligt att företag använder sig av standardavtalsklausulerna som finns för överföring av personuppgifter till tredje land. Det nämns inte mycket om dessa i förslaget, kan du berätta mer om hur dessa kan komma att påverkas?
7. Vi tycker att det är otydligt hur Binding corporate rules (BCR) fungerar idag. Kan

exempelvis ett IT-konsultföretag som har verksamheter i flera länder sluta ett avtal med en kund som hanterar svenska personuppgifter och sedan fritt överföra dessa uppgifter inom de länderna där koncernen har godkända BCR?

8. Hur har du tolkat att BCR kommer att påverkas av förslaget?
9. Har du noterat andra saker i förslaget som kan komma att påverka överföringar av personuppgifter till ett tredje land?
10. Tror du att det är sannolikt att förslagen kommer att förändras i någon större utsträckning innan de antas? På vilket sätt?
11. Anser du att påföljderna är rimliga? Om inte, vänligen utveckla.
12. Har du något annat att tillägga gällande ämnet?

Frågor till Peter Gerhard:

1. Vad är din generella uppfattning om förslagen? Vad hoppas man vinna, hur påverkar det Sverige och hur påverkar det andra EU-länder?
2. Enligt en artikel i Computer Sweden är Sverige ett av få länder som vill ha detta till ett direktiv istället för en förordning. Är detta korrekt? Varför?
3. Hur bedömer du variationerna i ländernas lagstiftning om det inte blir en förordning?
4. Varför tror du att det inte förs någon debatt om det här i Sverige?
5. Som vi har förstått det är det i dag vanligt att företag använder sig av standardavtalsklausulerna som finns för överföring av personuppgifter till tredje land. Det nämns inte mycket om dessa i förslaget, kan du berätta mer om hur dessa kan komma att påverkas?
6. Vi tycker att det är otydligt hur Binding corporate rules (BCR) fungerar idag. Kan exempelvis ett IT-konsultföretag som har verksamheter i flera länder sluta ett avtal med en kund som hanterar svenska personuppgifter och sedan fritt överföra dessa uppgifter inom de länderna där koncernen har godkända BCR?
7. Hur har du tolkat att BCR kommer att påverkas av förslaget?
8. Har du noterat andra saker i förslaget som kan komma att påverka överföringar av personuppgifter till ett tredje land?
9. Tror du att det är sannolikt att förslagen kommer att förändras i någon större utsträckning innan de antas? På vilket sätt?
10. Anser du att påföljderna är rimliga? Om inte, vänligen utveckla.
11. Har du något annat att tillägga gällande ämnet?

Frågor till person x på Heit:

1. Vad är din generella uppfattning om förslaget? Vad hoppas man vinna, hur påverkar det Sverige och hur påverkar det andra EU-länder?
2. Varför tror du att det inte förs någon debatt om det här i Sverige?
3. Hur och var i Heit förs det en dialog om förordningsförslaget?
4. Upplever ni att det är ett problem inom koncernen att dagens lagstiftning skiljer sig åt mellan

de olika EU-länderna där ni är aktiva?

5. Hur tror du att ni som koncern kommer påverkas av en mer enhetlig lagstiftning inom EU?
6. Hur ser Heit på BCR? Är det något som används eller har varit aktuellt att börja använda?
7. Hur ser Heit på att användandet av interna policys för att skydda information?
8. Anser du att Heits sätt att arbeta på med den tekniska lösningen, standardavtalsklausuler och certifieringar är ett vanligt sätt inom branschen att jobba på? Varför/varför inte?
9. Anser du att påföljderna i förslaget är rimliga? Om inte, vänligen utveckla.
10. Har du något annat att tillägga gällande ämnet?

Bilaga 2: Transkibering av intervju med Elisabeth Wallin

6/5 2013

EW: Elisabeth Wallin
HG: Henrik Georgson (intervjuare)

HG: Vad är din generella uppfattning? Vad hoppas man på att vinna? Hur påverkar det Sverige och övriga Eu-länder?

EW: Den stora vinsten man har velat se med den här förordninen är att man har velat få till en starkare harmonisering av dataskyddsbestämmelserna i de olika EU-länderna. För man har sett att även om det finns ett direktiv idag som sätter dom gemensamma målen så spretar ändå den nationella lagstiftningen lite för mycket har man tyckt. Och då vill man få en mer sammanhållen lagstiftning. Så det är det ena. Sen har man också velat förstärka den registrerades rättigheter ännu mer än vad som är idag. Det är väl dom två stora vinsterna.

HG: Och din uppfattning om det, är det rätt väg att gå tycker du? Ser du positivt på det hela?

EW: Ja. Att förstärka den registrerades rättigheter är ju något som vi stödjer. Och det är klart att det är bättre om man kan ha en mer likartad reglering över hela EU eftersom människor rör sig mellan länderna och så. Det är ju en bra tanke i sig. Sen så kan det finnas praktiska problem, dels när det gäller den här harmoniseringen så kan det finnas nationella bestämmelser på andra områden som gör att det kanske blir svårt att harmonisera just dataskyddsbestämmelserna så långt som man velat göra. Men tankarna är goda kan man väl säga men sen kan det bli vissa praktiska problem.

HG: Sen har vi då läst en artikel i Computer Sweden där det påstås att Sverige är ett av de få länder som vill ha det här till ett direktiv istället för en förordning. Hur ser du på detta? Stämmer det?

EW: Ja, det har funnits såna tankar. Sen vet inte jag hur långt... Det här förslaget håller ju på att förhandlas i rådet ... Det diskuteras också i parlamentet. I rådet så är det ju den svenska regeringens justiedepartement som företräder Sverige. Och jag vet inte exakt hur långt dom har drivit den frågan om att få det till ett direktiv istället. I början fanns det sådana tankar, det är helt riktigt. Det är inte Sverige ensamma om, det har funnits fler länder som har tyckt det.

HG: Precis. Men då, då är väl risken att man får en viss variation i lagarna och då tappar man väl lite poängen med det du sa att man vill ha mer harmonisering osv?

EW: Precis, det är det som står mot varann tycker jag.

HG: Vad ser du för för- och nackdelar där med dom olika alternativen?

EW: Ja, det är ju egentligen, det beror på vad man, det är klart att ett direktiv det får inte samma harmonisering. Och det är väl svårt att säga. Det är både bra och dåligt. Vissa fall så har varje land sånna nationella särdrag som gör att man måste ha mer skräddarsydda dataskyddsbestämmelser. Vi har ju i Sverige till exempel en stor mängd registerlagar som är särskilda personuppgiftslagar för vissa verksamheter, oftast myndigheters behandling av personuppgifter som vi har sett att det blir ett bättre integritetsskydd om man har skärddarsydda bestämmelser. Men det kommer, det är inte säkert att det fungerar tillsammans med den här harmoniseringstanken. Så det finns ju både för- och nackdelar med båda systemen.

HG: Om man då utgår från det förslaget som ligger, hur kommer Datainspektionen att påverkas av om förslaget träder i kraft?

EW: Vi som organisation tror jag inte kommer påverkas så mycket, rent storleksmässigt eller så. Eller vad vi har för befogenheter, det kommer nog i stort sett vara samma. Däremot är ju en tanke med förordningen att dataskyddsmyndigheterna i EU-länderna ska samarbeta mycket mer... Så där kommer det nog bli så att vi att vi har ännu mer kontakter med våra systermyndigheter ute i Europa.

HG: Och ett problem, potentiellt problem, är att företag har problem med att ställa om sig till det nya förslaget och de nya regler och lagar. Hur kommer då datainspektionen att göra för att underlätta för Svenska företag?

EW: Ja, i första hand är det väl en fråga om att informera om de nya reglerna när de väl är antagna. Det är den information som vi har då om hur man ska tolka och tillämpa dom regler sen så finns det väl egentligen inte nåt utrymme i förordning att för oss att meddela särskilda regler eller särskilda föreskrifter utan det blir mer information i så fall.

HG: Sen har vi då nästa fråga som rör de här standardavtalsklausulerna som används ganska flitigt idag. Det är ju inget som nämns i förslaget mer än att det kommer finnas, har du hört något mer om det eller vet du något mer om hur det kan komma att påverkas?

EW: Nja, det finns ju, ska se här, i artikel 42 i förslaget så nämner man att det är möjligt att överföra personuppgifter om man har apporiate safe guards heter det. Då finns det artikel 42.2.2b så pratar man om de här standard data protection clausuls.

HG: Det nämns inte så mycket om hur dom kommer att påverkas eller om man kan fortsätta använda dom man har idag eller hur det komer att se ut.

EW: Nja, men det är nog tanken att man ska kunna fortsätta göra det. Det har man nog utgått ifrån.

HG: Då kommer vi även in på BCR. Det verkar ju vara lite otydligt hur det fungerar idag och hur det kommer att påverkas. Vad vi har läst förenkla det så att företag kan använda det i större utsträckning. Men det inte framgår exempelvis om BCR kan användas som stöd för överföring till tredje land om man har en kunds uppgifter. Om du förstår vad jag menar.

EW: Mm, alltså. BCR var från början tänkt att hanteras inom en koncern. För att man ska kunna föra över uppgifter inom koncernen. Och det är då det man har i de flesta BCR som har godkänts. Eller så gott som alla, har gällt sådana överingar inom en koncern. Sen så har alldeles nyligen dataskyddsmyndigheterna i EU börjat fundera på om man kan godkänna BCR för koncerner som agerar som personuppgiftsbiträden. Ehh. Men då är fortfarande tanken att BCR bara ska vara inom koncernen. Så ett biträde som då får ett uppdrag från någon annan att hantera uppgifterna. Det uppdragsledet måste ändå regleras på något annat sätt, genom standardavtalsklausuler till exempel. Men så just BCR där är tanken att det ska vara inom en koncern.

HG: Och hur har du tolkat att det kommer påverkas. BCR. För att som vi ser det så är det inte några jätteskillnader jämfört med vad som finns idag. Mer än att dom säger att det ska bli bättre liksom.

EW: Det man kan tycka är bra med förordningen är att man nu nämner BCR och erkänner det uttrykligen som en sån här garanti. Idag i direktivet så finns det ju inget som heter BCR i någon artikel i direktivet utan man, det finns en bestämmelse om man har tillräckliga garantier och då är den bestämmelsen man har tillämpat och ansett BCR då kan utgöra tillräckliga garantier. Nu nämner man det mer uttryckligen i förordningen och har det mer tydligare att man ska kunna använda sig av dom och vad som ska gälla för såna regler.

HG: Har du noterat några andra saker i förslaget som kan komma påverka överföringar till tredje land så att säga?

EW: Nej. Vi hade väl en synpunkt i vårt remissyttrande från mars i förra året. Precis när förslaget hade lagts så skickade svenska regeringen ut det på remiss till olika instanser. Då tyckte vi, tolkade vi dom här bestämmelserna om trejde landsöverföringar som att man inte längre själv kan göra nån bedömning om det finns en adekvat skyddsnivå eller inte. Som personuppgiftslagen och direktivet är formulerat idag så finns det ett stycke som säger vilka omständigheter man ska ta hänsyn till innan man gör en bedömning om ett land har adekvat skyddsnivå eller inte. Då har vi tolkat det som att i princip kan man göra den bedömningen själv, sen har ju kommissionen då när det gäller vissa länder fattat beslut om att de har en adekvat skyddsnivå och då är det ju klart och tydligt. Men det har inte funnits något som har hindrat att man har gjort den bedömningen själv. Även om det är en svår bedömning att göra. Och den möjligheten har inte vi sett i det här förordningsförslaget. Sen kanske

det inte får så stor praktisk betydelse ändå eftersom att det är en svår bedömning att göra själv som personuppgiftsansvarig. Men det är våran synpunkt som vi har i vårt remissvar iaf. Annars har jag inte sett några stora förändringar.

HG: Intressant. Hur tror du att förslaget utvecklas och förändras innan det antas? Hur har du uppfattat att debatten går omrking det så att säga?

EW: Ja... Just nu så är det ju ganska mycket disskusion om rätt många olika saker. Det har ju varit en disskusion i parlamentet, i ett utskott där och det har funnits väldigt många ändringsförslag. Så att det är svårt att sia om hur det kommer att se ut till slut. Det kommer ju inte se ut precis som det gör nu. Det kommer att komma ändringar, det tror jag säkert.

HG: Vi har ju läst vad som finns att läsa om det här och väl sett att det finns lite politiska synpunkter som bl.a. menar på att amerikanska storföretag försöker urvattna förslaget. Vad har du för synpunkter på det? Är det nånting du har hört och tagit ställning till?

EW: Nwj, det känner jag faktiskt inte till. Jag har mest tittat på den här diskussionen i parlamentet och rådet och dom olika tankar man har där. Jag har inte riktigt sett det du pratar om. Det kan hända att det finns.

HG: Sen är det då påföljderna som har blivit lite strängare. Tycker du att dom är orimliga eller rimliga?

EW: Dom kan mycket väl vara rimliga. Det vi har saknat både Datainspektionen och andra dataskyddsmyndigheter är ju att vi kanske hade velat se ett utrymme för oss att avgöra om det ska utdömas böter eller inte. Som bestämmelsen är utformad nu så är den ganska absolut. Har man gjort en viss överträdelse ska man får betala böter. Men vi hade velat att det skulle bli upp till dataskyddsmyndigheterna att avgöra om vi ska utdöma böter eller inte.

HG: Okej. Har du något annat att tillägga i det här ämnet? Framför med fokus på tredjelandsöverföringar?

EW: Nej, jag tycker det ska bli spännande att se hur det utvecklas och hur det slutar. Det är som sagt väldigt mycket diskussion. Vi får se hur det blir.

HG: När bedömer du att det här kan vara klart och när kommer det här att börja gälla som förordning tror du?

EW: Tanken är att... Den plan man arbetar efter är att det här ska vara klart och antaget i nästa parlamentsval, vilket alltså är i första halvan av nästa år. Sen har då medlemsstaterna två år på sig att

genomföra förslaget. Att se till att det genomförs i nationell lagstiftning. Så det är allltså 2016. Det kan man nog säga är det tidigaste.

HG: Då har vi fått våra frågor besvarade och tackar för intervjun.

Bilaga 3: Transkibering av intervju med Amelia Andersdotter

6/5 2013

AA: Amelia Andersdotter
HG: Henrik Georgson (intervjuare)

HG: Vad är din generella uppfattning om förslaget och vad ser du att man kan vinna på det, hur påverkar det sverige och hur påverkar det övriga europa?

AA: Ja vi behöver uppdatera personuppgiftslagstiftningen. Den är inte alls tidsenlig och den har inte haft dom effekter vi vill att dataskyddslagstiftningen skulle ha i Europa så att det har funnits ett behov av en reform har varit ganska uppenbart under väldigt många år redan men det är ett ganska stort område att reformera och därför har det dröjt med att ta fram ett förslag för det krävs mycket politiskt mod att lägga ett sånt förslag … Det "direktorat" på kommissionen som egentligen har ansvar för mänskliga rättigheter har väl gjort ett förhållandevis bra jobb med att göra en ny förordning men sen har det varit många kompromisser på vägen fram till att förslaget faktiskt lades som gjorde att kommisionens förslag kanske inte blev så bra ändå. Dessutom har man nischat några av dom erfarenheter som då har gjorts av dataskyddslagstiftning hittills när man forskar på profilerng och så där och då kommisionen kanske nischar för att de "mål" av personuppgiftslagstiftning har givit alldelse för stort utrymme för privata aktörer att behandla en massa personuppgifter på skumma sätt utan att berätta det för någon t.ex och då vet vi liksom inte inte ens vad som är relevant att reglera i den privata sektorn.

HG: Det kom en artikel i CS för några dagar sen och där skriver dom ju då att sverige vill ju ha detta som ett direktiv istället för en förordning stämmer det fortfarande och varför är det i så fall så?

AA: Problemet för Sverige är ju att Sverige inte har någon ambition om att vi faktiskt ska ha privatliv. Svenska regeringen har inte tänkt igenom detta ordentligt utan man tänkter spontant att det är bättre med ett direktiv än en förordning. Så får vi skriva en svensk lag men sen tänkte vi inte på att vi inte kan upprätthålla den svenska lagen i sverige och då har, t.ex jurister på stockholms universitet, som har jobbat med dom som var aktiva i puldebatten i sverige i mitten av 1990-talet, och dom tänkter så här: Vi har ju en massa specialregisterlagar i sverige som reglerar sjukvården och arbetsförsäkringar och allt sådant där seperat och då kan man ju garantera jättemycket variabelt integritetsskydd. I varje offentlig myndighet det blir jättebra men nu när vi har börjat införa it-system i all offentlig administration som oftast inte utformats eller görs av aktörer som den offentliga sektorn själv kontrollerar eller kan verfiera resultaten för då lyder ju inte dom under den här sektorspecifika eller institustionsspecifika regleringen

som man har i sverige. Utan då har man skickat ut all offentlig data i nån form av juridiskt ingen mans land. Då frågade jag stockholms universitet hur tycker ni att man ska lösa det här då? Ja man kanske ska tänka sig för innan man börjar digitalisera offentlig verksamhet säger dom då och det är visserligen ett gott råd men det har vi ju inte gjort utan nu är ju situationen den att all administration i offentlig verksamhet ligger på en massa privata aktörer som eventuellt inte är baserade i sverige och som därför inte faller under vår personuppgiftslag eller någon specifik registerlag och det kommer nog bli väldigt svårt för oss att ändra på det annat än att bryta mot till exempel värdshandelsorganisationens upphandlingsregler. Så känns det, för mig iallafall, men det är ju kanske så att politiker har ju genomfört en massa förändringar i hur vi hanterar data i samhället dom senaste 10 åren som dom inte fattar vad det innebär för lagstiftningen och nu förstår man inte att nu när vi har gjort alla dom här förändringarna för att vi ska uppnå dom här politiska målsättningarna vi har så behöver man ha en reglering som kommer åt hur privat sektor hanterar data. detta är personuppgiftförordningen dataskyddsförordningen på eu-nivå för det är så många aktörer annars som inte är baserade i sverige som inte går att komma åt effektivt med vår egen lagstiftning. Man behöver hela unionens ekonomiska tyngd bakom det här samt ett regelverk som väldigt tydligt ställer just offentlig verksamhet och privat verksamhet på lika villkor och jag tror att det där är bara för att vi helt enkelt har en väldigt omogen politisk debatt om det här vi vet liksom inte att vi har skrivit på en kommision där privatliv är en grundlägggande rättighet. Vi vet i sverige att man har haft mycket konfliker mellan medborgare och F.R.A t.ex men sen när det gäller så här lite djupare funderingar kring hur hanterar vi hela vår administrativa infrastruktur? Där har man liksom inte kommit ikapp egentligen politiskt utan man har inte fattat vad det är för förändringar man genomför. Det är ju genomgående så. Vilken politiker är ansvarig för hur apoteket hanterar dina personupggifter? Nämn en politiker som skulle kunna vara det. På vilken nivå sitter den politikern. Nationell, landsting, kommunal nivå? Gör en gissning. Det är sådana frågor som vi inte har kontroll över när det gäller privatliv och politikerna vet inte heller och har ägnat jättemycket tid åt att undvika ansvar framförallt.

HG: Så politikerna vet för lite då kan man säga ?

AA: Det finns ingen offentlig debatt och det finns inget intresse för att det förs nån debatt heller känns det som. Vi skulle naturligtvis behöva prata om mycket mer. Vem bör vara ansvarig och för vad och hur ska det ansvaret utdelas? Det är sådana saker som vi uppenbarligen behöver lösa mycket bättre och där kan man ju tänka sig då att kommisionens förslag gör en ansats för att ta hand om den frågan men det är inte bara i dataskyddsförordningen man behöver ta den disskusionen om dom här områdena. Utan det är en massa annan lagstiftning också och kommsisionen har fegat och inte gått tillräckligt långt för att dom står under hårt tryck från kommersiella intressen precis som alla andra. Regeringen fattar inte vad dom håller på med och parlamentet är extremt känsligt för stora lobbypåtryckningar så framförallt när vi då saknar en kontrollerad samhällsdebatt och resonemang kring vad det är vi håller på med så då blir det liksom väldigt svårt att få en vettig lagstiftning egentligen.

HG: Men om det skulle bli ett direktiv istället för en förordning hur bedömer du att variationerna med ländernas lagstiftning kan bli då är det ett stort?

AA: Ja men det kommer inte bli det. Det finns inget stöd för ett direktiv. Kommissionen stödjer inte det, parlamentet stödjer inte det. Merparten av regeringarna i ministerrådet stödjer inte det. Regeringen rekommenderade riksdagen att föreslå att det skulle bli två direktiv eftersom regeringen är van vid att föreslå sådana saker när det kommer en förordning och då sa riksdagen att: Ja det låter bra att vi får en egen lag i sverige och sa ja till det och nu vill regeringen då ändra risksdagens ställningstagande. Det kommer inte bli två direktiv. Det är bara att köpa det

HG: Och hur kommer Piratpartiet att jobba med förslaget fram tills att det träder i kraft?

AA: Jag försker ju få en starkare personuppgiftsförordning än den kommissionen har föreslagit. Jag vill ju ha ett starkt dataskydd i europa och att vi som medborgare har möjligheten att säga ja eller nej till hur våra personuppgifter behandlas och jag tycker också vi behöver skapa mekanismer för att vi behöver skapa incitament för konkurrens med privatlivsfrämjande teknologier. Vi behöver alltså reglera den här sektorn på ett sådant sätt att det bästa ett företag kan göra är att vara mer privatlivssäkert än ett annat företag istället för tvärtom så att man får konkurrensfördelar av att ta tillvara på medborgarnas självbestämmande anonymitet och det är ju sånt som politiker kan göra om dom vill. Vi har ju jättemycket makt att sätta upp dom interaktionsstrukturer vi vill ha i samhället och det tycker jag att den interaktionssruktur som jag tror att dom flesta männsiskor vill ha är en när dom själva har kontroll över sina liv på något sätt och över sina bekantskaps. Att man själv bestämmer hur man interagerar. Under vilka villkor att man inte blir ständigt övervakad och tittad på och på något sätt tryckt till att agera på ett särskilt sätt. Så det har jag försökt göra. Det finns ju en massa specifika grejer som jag tycker är extra viktiga i olika artiklar och så där men det kanske är mindre intressant. Den idelogiska tanken jag har bakom är att dom flesta människorna mår bäst av att ha makt över sitt liv.

HG: Och vad kommer du och Piratpartiet göra för att få igång debatten här hemma i Sverige?

AA: Vi försöker lägga debattartiklar och skicka pressreleaser och så där. Nu har Dagens industri och en massa andra tidningar, senast igår, skrivit att amerikansk industri försöker urvattna europeisk dataskyddslagstiftning. Det är ju en sanning med modifikation för amerikansk industri kan ju inte skriva europisk lag utan det är ju europeiska lagstiftare som gör det. Så då har jag identifierat att Anna-Maria Corazza Bild, från Moderaterna, verkar ha lagt många av den amerikanska industrins lobbyförslag och då tycker jag att det faktiskt är Moderaterna som urvattnar europeisk lagstiftning. Det är dom som har mandat att göra det och det är dom som gör det och dom har valt att lyssna på den amerikanska

industrin och nu verkar det inte som att media är så intresserade av att plocka upp den iden. Så det är ju tråkigt att man ställer en folkvald ledamot till svars för dom politiska förslag man faktiskt lägger i församlingar men vad vet jag? Det kan ju vara så att dom har en genomtänkt vision bakom att stödja just den amerikanska it-industrin. Det är ju kanske så att den amerikanska industrin helt enkelt ses som mer värdefull än grundläggande rättigheter av moderaterna och att dom har ett sunt resonemang bakom det. Det har media då inte heller låtit Moderaterna ge uttryck för i svensk media vilket jag tycker är synd. Det kanske är så att vi inte vill ha privatliv i samhället också. Det kan ju vara så att piratpartiet har fel men för att vi ska få reda på det så måste vi ha en debatt först och vi försöker starta det men var ska man börja?

HG: Om vi då går in lite mer specifikt på förslaget i sig då. Så kollar vi då lite mer specifikt på vad som händer när man för över till tredje land. Vilket då är väldigt vanligt idag och då använder man sig av någonting som heter standardavtalsklausuler och det nämns inte så mycket i förslaget mer än att, ja, det ska finnas... Hur har du uppfattat just den detaljen hur kommer det påverkas?

AA: Det där är ju en väldigt känslig fråga men från artikeln i kommisionens ursprungliga förslag fanns det innan. Alltså inte det första förslaget som faktiskt lades, utan det förslag som gick i kraft, ville lägga innan dom skickade ut det till andra delar av kommisionen för reveiw och sen det förslaget det blev där fanns det en artikel 42 som satte in väldigt bra kontroller över när man får överföra data och inte. Problemet här är ju då att t.ex med USA har man ju gjort en massa specialöverföringsavtal till exempel SWIFT. Så innan vi har beslutat hur vi faktiskt hanterar personuppgifter på europeeisk nivå har vi bara skrivit en massa avtal med USA om att skicka över en massa persouppgifter dit och nu håller man på med liknande grejer att man sluter avtal med USA om hur vi ska åsidosätta vår egen lagstiftning innan vi bestämmer vad vi tycker att vår egen lagstiftning ska vara. Så binding corporate rules, ni tycker det är otydigt hur det fungerar idag. Det korta svaret är väl kanske att det beror på vilket mål du har om du tycker att det ska finnas ett personuppgiftsskydd så fungerar dom ju inte. Det är ju så. Dom ger ju inte personuppgiftsskydd. Det är ingen skyldighet på företagen där att göra nånting, så det är en sak då som förslaget försöker strama upp lite grann och det blir bättre kontroller av binding corporate rules i kommissionens förslag i det förslag som låg på kommissionens bord. Innan dom offentliggjorde det så var det ännu hårdare kontroller på binding corporate rules men jag tycker att man kan inte bara säga att företag får skriva avtal med sig själva om hur duktiga dom är på att skydda privatliv. Däremot ska det finnas combined mechanisms i artikel 58 i förordningen och det måste finnas nån form av granskning och kriterier på vad dom här binding corporate rules ska göra och inte göra. Standardavtalsklausuler för överföring av personuppgifter till tredje land tycker jag som regel att man inte bör få ha faktiskt men då är problemet att du har ännu större problem där. För vad dom gör nu i europeisk industri är så här, dom får ju inte överföra datan till tredje land så då lägger dom datan på en europeisk server och sen hyr dom ut hela maintence av databaserna på indier som då loggar in på dom svenska servrarna remotely men

det gör ju liksom att datan ändå på nåt sätt måste göras tillgänglig i Indien och då har vi ju samma säkerhetsproblem ändå. För egentligen bör man nog fundera över om det är så jävla bra att lägga över t.ex. medcinska journalen på system till en som ska hanteras av indier i Indien.Vvi kanske inte vill att det ska finnas en indisk infrastruktur som kommer åt alla dom här personuppgifterna eller ett lite mer enkelt fall kan man komma åt det från Indien, ja då kan man ju komma åt det från Turkiet också och är man till exempel en svensk kurd då kanske man inte vill att turkarna ska sitta och komma åt ens medicinska journaler på håll. Det är ju såna saker som förslaget inte riktigt löser där man egentligen skulle behöva annan lagstiftning också och tydligare lagstiftning där vi kanske behöver gå in och titta på hur man hanterar offentlig sekretess i olika system och vad är det rimligt att digitalisera och inte. Det är ett landsting i Sverige som har utfört utredningar om hurvida man ska lägga journaler på nätet eller inte och om det är rimligt att sjukhurpersonal använder Facebook på internetupkkopplade datorer som också kommer åt medcinska journalsystem det är Jämtland. Dom kom fram till att det inte var så bra om personalen använde sociala medier på samma datorer som dom kommer åt medcinska journaler med. Myndigheten för samhällsskydd och beredskap rekomenderade att medicinska journaler inte ska ligga på nätet men varken Stockholm, Uppsala eller Skåne har av detta dragit slutsatsen att man kanske inte ska lägga journaler på nätet utan dom tycker att det är jättebra med digitalisering. Trots att läkare i till exempel Uppsala läns landsting inte tycker att det är en bra idé. På Karolinska sjukhuset så har man säkrat dom medicinska journalerna med ett lösenord som sitter på en post-it lapp i en korridor så att personalen kan komma åt journalerna när dom kanske måste och då har man för att skydda det lösenordet infört fotoförbud i korridoren och det är liksom så fungerar medicinsk läkarsekretess i Sverige idag. Här är det ju liksom ett mycket större skydd än personuppgiftslagen men personuppgiftslagen skulle iallafall ge någon form av ekonomiskt dataskydsförordningen ger något ekonomiskt ansvar på dom som bygger it-systemen så att om dom failar och nån bryter sig in på deras system så blir dom iallafall skydliga att betala en jäkla massa pengar för det och det är ganska rimligt tycker jag. Och då kan man egentligen säga att det är ju inte så mycket pengar bara 2% av omsättningen. Vilket är sex gånger så lite som man betalar till exempel för konkurrensöverträdelser, så även där har ju egentligen kommissionen varit väldigt väldigt försiktig kan man säga. Det borde egentligen vara hårdare sanktioner mot företag som beter sig dumt. Det är sannolikt att förslagen kommer förändras i någon större utsträckning. Ja det har varit jättehårt lobbytryck och det finns inte en jävla ledamot som vet vad dom håller på med. Det är ganska stor risk att det blir stora förändringar. Sveriges regering fattar egentligen inte heller vad som är tror jag eller säg det finns inget tydligt mål i samhället att bevara privatliv vi har i rättighetskatalogen i europeiska kommissionen för mänskliga rättigheter och det är en grundläggande rättighet men om du tittar på typ till exempel hur myndigheten för samhällsskydd och beredskapser på sitt it-certiuppdrag så ser dom det som ett av deras målsättningar är att dom ska skydda mänskliga fri- och rättigheter samt privatliv. Vilket betyder att då har man lagt privatlivet utanför den egentliga rättskatalogen för då har liksom den riktiga i rättskatalogen i den som det står om dom fri- och rättigheter som vi egentligen har och sen har vi privatliv som egentligen inte hör

till där men som man lägger till som appendix. Så ska det ju inte vara, deras uppdrag borde ju vara mänskliga fri- och rättigheter särskilt privatliv privatliv är en mänsklig rättighet i Europa. I USA är den inte det, i USA är det en konsumenträtt och det är en stor skillnad i hur man stiftar lagar och vilka skyldigheter man kan säga att staten har gentemot medborgare. I olika sammanhang och inte om det är en konsumenträtt så är det ju liksom något som bör i princip regleras mellan marknadsparter konsument och försäljare. Om det är en mänsklig rättighet så har staten ett moraliskt ansvar att säkerställa att medborgarnas privatliv upprätthålls även gentemot privat sektor. Skulle jag argumentera … men vi har liksom inte riktigt den insikten i den politiska debatten idag utan vi har liksom inte, vi vet inte, jag vet faktiskt inte hur man ska se på det så att vi vill träda ur Europiska Kommissionen för mänskliga rättigheter och det kan ju ses som ett legitimt politiskt val i och för sig. Vi behöver inte vara medlemmar i den kommissionen men det känns som en samhällsdebatt som vi isådana fall borde ta innan vi skriver om personuppgiftslagstiftningen på ett sätt att den inte skyddar personuppgifter och det har vi liksom inte gjort och det verkar inte som att det finns någon som fattar att den här jättestora skillnaden mellan USA och EU … i rent privatliv … i samhället gör skillnad det är en jättestor filosofisk skillnad mellan hur man bygger rättssystem om man ser saker som grundläggande rättigheter eller som konsumenträttigheter för i EU så är ju konsumenträttigheter typ att om Ikea säljer dig en trasig stol så måste dom byta ut den. Det är ju en konsumenträttighet så det är ju skillnad om man ser privatliv som jämmställt med att få sin trasiga stol utbytt eller som någonting som grundläggande för att vi faktiskt ska kunna delta i demokratiska system.

HG: Har du nåt annat att tillägga om vi kollar lite mer specifikt på det här med tredje lands överföringar har du någonting annat som du har funderat på kring det förslaget?

AA: När det gäller dataskyddsförordningen är ju så här vi måste lära oss säga nej till USA. Vi behöver inte säga ja till dom helt enkelt.

Bilaga 4: Intervjusvar Heit

17/5

1.
Vi för bättre kontroll på hur vi hanterar denna typ av information och gemensamma regler EU Förslaget är bra. Det ger en större förståelse för problematiken kring behandling av personuppgift.

2.
Individen själv begriper inte vad som kan göras med den information som är samlad. Problemet att ingen förstår konsekvenser av behandlingen och hur detta påverkar mig som medborgare.
Oftast hänvisas till det förhärskande ”rent-mjöl-i-påsen” uppfattningen, vilken är en skymf emot den mänskliga rättigheten till ett privatliv.

3.
Förs […] på Corp. Nivå. Skadan på varumärket och storleken på böter!

4.
Problem att anpassa produkten till olika nationella lagstiftningar.

5.
En ökad medvetenheten och öka förståelsen i affärsgränssnittet både hos oss våra kunder. Ökad förståelse för problematiken i affärsgränssnittet.

6.
Vi vill gärna se oss som användare BCR men värdet är begränsat

7.
Policyn måste ju finnas detta är ett viktigt styrmedel. Vi får inte heller komma i en situation med för många policyn. Det måste finnas en bar koppling med verkligheten och möjligheten att kunan göra affärer.

8.
Ja, det finns inte så många andra möjligheter att hantera detta på om man är medveten om problematiken. Det ökar förståelsen mellan kund och leverantör. Det är mer eller mindre ett krav från våra kunder att vi har ISO 27000 och ”kör” enligt ITIL.

9.
Ja det skall vara enkelt att döma ut straffet och beloppet och dom är rimliga. Förhindrar långa domstolsförhandlingar och allehanda jämkning av bötesbeloppet. Ökar därigenom trovärdigheten i lagstiftningen.

10.
Gallring, Hur skall företagets kontrollmekanismer se ut för att vi skall följka denna lagstiftning.

Bilaga 5: Transkibering av intervju med Peter Gerhard

20/5 2013

PG: Peter Gerhard
EK: Emil Kristiansson (intervjuare)
HG: Henrik Georgson (intervjuare)

HG: Fråga ett, vad hoppas man vinna?

PG: Trygghet för individerna. Alltså. Och visa en slags handlingskraft. Jag vet inte om individerna blir så mycket tryggare men det vill jag hoppas på. Det man hoppas på men jag tror inte det blir så mycket större, det skyddet. Och så vill man visa handlingskraft. Sen är det så när en teknisk, när tekniken växer så släpar ju juridiken många år efter. Det gör den ju i all lagstiftning. Och då försöker man i efterhand lappa och laga. Alltså istället för att när man märker när något nytt håller på att hända inom något tekniskt område som här så ska lagen gå före och tala om att så här vill vi ha det. Då kanaliserar man hela, alla företagens beteende. Här gör man precis tvärtom, man kommer i efterhand. Nu gör företagen redan på ett visst sätt. Jaha. Då ska vi försöka ändra det här och styra om det. Då är man väldigt sent ute. Så på frågan vad man hoppas vinna. Det är en trygghet, det är det naturligtvis. För att skydda individen... Sen på tvåan står det inget... Trean står det, direktiv istället för förordning. Ja, det är ju mindre styrning med ett direktiv och det gillar vi i Sverige. För vi tycker att vi ligger långt fram inom det här området. Vi var först i världen med en datalag, tror jag, när den kom. Så vi tycker att vi ligger långt fram. Så det räcker för oss att ha ett mål så kan vi själva se till att det uppnås medan alla andra länder. Ja, dom kan väl tycka att en förordning med detaljstyrning är enklare så slipper dom hitta på så mycket själva, då kommer alltihop färdigt. Så vi är nog generellt sett mer för direktiv istället för förordningar. Vi har ett väl utvecklat rättssystem. Vi tycker att vi kan skapa detaljreglerna själva och dom behöver inte EU visa.

HG: Men då är ju frågan hur variationerna blir om det skulle bli en förordning. Kommer det bli stora skillnader i lagarna så att det blir svårt för företagen att använda sig av förordningen?

PG: Ja, det blir det oavsett. Hur bedömer du variationerna i ländernas lagstiftning om det inte blir en förordning? Ja, dels är det ju lagstiftningen, det är ju en sak. Sen är tillämpningen faktiskt en annan sak. Hur fint det än står i lagarna så om du tittar på tillämpningen så tillämpar man de här reglerna eller inte? Eller är det bara en symbol som sen tillämpas på annat sätt? Där finns också en stor diskrepans som är intressant att se. Det kan man ju se på lagen om offentlig upphandling, dom lagarna har jag ägnat mig mycket åt. De ska ju gälla inom alla EU-länder och alla tycker att dom är jättebra, för att dra en parallell. Italien tycker att dom är jättebra men dom skiter fullständigt i dom. Då kan man väl säga att ja, variationerna i lagstiftningen är inte så stor. Men variationen i

tillämpningen är stor. Så där finns ytterligare en dimension som gör det besvärligt. Så svaret är att jag bedömer variationerna mindre om det är en förordning. Dom blir större om det blir ett direktiv men därmed har man inte uttalat sig om tillämpningen. Om ni förstår vad jag menar. Så där är en intressant skillnad också… Varför tror du inte det förs någon debatt? Jag tror att det är för tekniskt. Det tror jag. Alltså en öppen debatt har vi fört om upphovsrätten och jag tror att folk är trötta på det här. Det förstår inte tekniken riktigt och vad det handlar om. Så, men det kan vara lite förvånande. Det handlar ju om individens skydd.

EK: Det är ju många som är berörda.

PG: Ja, men jag tror att det är så tekniskt svårt. Det krävs rätt mycket för att sätta sig in i det här. Det har ni ju märkt. Ni kan ju fortfarande inte svara på alla frågor man skulle vilja ställa. Om man går in på detaljer och det är kanske ingen som kan svara på det. Det är klart man kan ha en generell uppfattning om att det här måste regleras för att skydda mig. Men samtidigt så finns den andra sidan att nu växer byråkratin mer och mer och handlingsutrymmet minskar. Det finns ju både fram och baksida. Men jag tror att det är för tekniskt komplicerat och okänt, det tror jag att det är... Fråga nio, är det vanligt att företag använder sig av standardavtalsklausuler som finns. Det nämns inte mycket om dessa i förslaget. Jag vet faktiskt varför de inte nämns så mycket och hur de kommer att påverkas. Det vågar inte jag svara på.

HG: Nej, för att när vi läste förslaget, var vi förvånade. Det står bara att man kan använda dom. Det är ju stor skillnad på om man måste göra nya avtal med nya avtalsklausuler eller om de befintliga blir gällande.

PG: Det borde dom inte bli det. Om man nu tar ett steg framåt för att skydda. Då borde man inte behålla det gamla för då har inte det steget tagits där.

HG: Precis, eller så är dom så välutvecklade och välformulerade.

PG: Det tvivlar jag på men så kan det vara. Visst kan det det.

HG: Det är väl också de indikationer vi har fått från annat håll. Att man tänker att man kan använda dom och att de fungerar bra.

PG: Vem är det som säger det?

HG: Elisabeth Wallin på Datainspektionen, hon är jurist.

PG: Ja, det borde ju hon veta.

HG: Jo, men vi blev lite konfunderade.

PG: Jag vet inte om jag håller med henne men hon är ju mer insatt än vad jag är. Men det betyder ju inte... Hon är kanske diplomatisk. Hon representerar ju staten. Slår ni upp det så kan det bli nyhet av det om Datainspektionen inte tror på. Det vet jag inte, det är bara jag som spekulerar.

HG: Det är väl otydligt där tycker vi.

PG: Ja, jag kan inte tillräckligt mycket om det. Men jag skulle tänka mig att dom behövs göras om och att de behöver skärpas. Men det är bara som jag tror... Fråga 11, vi tycker det är otydligt om de här BCR-reglerna fungerar. Det vågar jag inte heller svara på. Faktiskt är det en jättesvår fråga, jag vet inte.

HG: Det är också lite sådär beskrivet i förslaget samtidigt som alla verkar väl införstådda med hur det kommer bli. Framför allt Wallin på Datainspektionen.

PG: Vad säger hon?

HG: Hon säger att det kommer bli enklare och att fler företag ska kunna använda dom faktiskt. Men om det faktiskt blir någon skillnad, det har vi svårt att utläsa ur förslaget.

PG: Så det blir samma på nästa fråga. Jag vet inte. Har du noterat andra saker som kan påverka överföring av personuppgifter till tredje land? Nej, alltså det bör ju bli lite svårare eftersom om tryggheten och skyddet ska öka bör det ju bli en belastning och svårare. Men jag tror inte så mycket på såna här. Jag har ju sett hur det funkar idag med överföring till tredje land och det svamlet som är i lagen och den motivering till det man ändrade då för många år sen, den paragrafen för hur det skulle bli lättare att överföra till tredje land. Det fick man inget riktigt svar på och jag hade kontakt med Datainspektionen och frågade hur de hade tänkt sig. De kunde inte svara. Tillfredställande nivå? Ja, vad är det för nånting? Det är beskrivet som att man ska kunna skicka det vart som helst utan att det ska hända något, ungefär så. Ja, jag har jättesvårt för det. Alltså jag vet att jag är kritisk mot sånt här. Men det är svårgreppbart, sen har jag en känsla av att EU vill visa att "vi tar hand om allt och vi är aktiva, vi agerar och vi reglerar". Men sen stannar det lite där. Tillämpningen och praktiken är en annan sak. Det skapar en oerhörd byråkrati. De företag som skiter i det, de klarar sig ofta undan.

HG: Nej, vi har ju inte hittat något rättsfall där ett företag har påverkats. Eller blivit fällt för nån överträdelse.

PG: De är okunniga och struntar i det. De kör på tills de får påpekande. Ja, sen får de inga påpekanden. Tror du att det är sannolikt att förslagen kommer förändras i någon större

utsträckning? Ja, i så fall att det blir fler undantag.

HG: Alltså att man börjar smalt?

PG: Ja, tratten blir ännu vidare. Dom får in så mycket "så kan inte vi göra" och då blir det "nej det är klart, då lägger vi in ytterligare". Det kan jag tänka mig att det ändras. Alltså att det blir mer uttunnat. Det är svårt när man lagstiftar, att skriva en lag för en verklighet som är så mångdimensionell och när det handlar om mycket pengar. Och en handel som ska fungera. Alltså att styra det med regler är jättesvårt. Jättesvårt. Det gäller ju alla områden. Det gäller ju här. Fler undantag kan jag tänka mig… Anser du att påföljderna är rimliga? Det är samma sak där. Vad som står i lagen är en sak och vad som döms ut eller händer i verkligheten är en annan sak. Tillämpningen... Alltså är det farligt att bryta mot en lag? Ja, enligt lagen kan det vara farligt men i praktiken händer det inget.

HG: Nu står det ju klart och tydligt i förslaget, nu kan man få upp till 2% böter. Av företagets omsättning. Det är mer det vi undrar. Är det en rimligt? Vi har fått andra indikationer som menar på att det här är ganska lågt om man jämför med andra lagar.

PG: Jämför du med konkurrenslagen så ligger den på 10 % och då kan det vara hela koncernens omsättning. Så det kan bli våldsamma belopp men det döms ju aldrig ut men 2% verkar lite mesigt. Varför drar man inte en parallell till konkurrenslagen då? Som ju också är internationell på det viset. Så det håller jag med om men sen kan man säga att det spelar ingen roll vad man sätter för procentsats, för det ju döms ju inte ut några höga belopp ändå. I konkurrenslagen har det ju dömts ut höga belopp men aldrig så högt som 10 %. Men hur motiverar man 2 %? Vet ni det?

HG: Det framgår inte i förslaget hur dom har kommit fram till det.

PG: Idén till det finns ju sedan tidigare. Det tycker jag är intressant generellt, att förr på den gamla goda tiden kunde man få böter om man bröt mot något. Böter är ju alltid låga så det går ju inte få höga böter. Sen kom man ju på att "vi skulle kunna döma högre böter men då kallar vi det för avgifter istället, så då pratar vi företagens språk. Då är det pengar som gäller". Det tycker jag är intressant att man går över till avgift, sen är det en intressant tanke att man kan dömas till att betala en avgift som är baserad på omsättningen och att man slopar den gamla bötesregleringen. Men det är möjligt att man har tänkt så här "man dömer ju aldrig ut 10 % i konkurrenslagen, det händer ju inte. Då kanske vi ska sätta en realistisk gräns på 2 % istället". Sen om den används så kan man öka den gränsen. Kanske har man tänkt så. Men man kan ju också tänka så om man är lite negativ "Ja, det spelar ju ingen roll för att det är så få företag som blir dömda". Så det är intressant som ni gör för det finns så mycket att ta hänsyn till och diskutera. Men skulle man vara ansvarig för det här och ha som jobb att skriva en sån här lag skulle jag tycka var alldeles för förlig. Fy fan. Alla dessa undantag. Det blir mer och mer undantag. Sen om ni tittar på exempelvis hur svårt det är att skriva så står det i artikel 42 "lämpliga skyddsåtgärder enligt punkt 1 kan bland annat ta formen av

bindande företagsregler enligt 43an". Så går man till 43an, där finns inget om företagsregler. Där heter det företagsbestämmelser. Det är ett helt annat uttryck. Kan de inte ens skriva så att det här blir harmoniskt inom det här. Då säger man som jurist "Företagsregler, ja här finns inga bestämmelser om företagsregler men här finns bestämmelser om företagsbestämmelser". Ja, då kan man ju säga att det inte är någon skillnad på det men båda begreppen används ju. De hänvisar ju till något som inte finns. Har ni märkt det också?

HG: Ja, det är lite rörigt och svårt att hänga med.

PG: Det visar ju hur svårt det är att skriva det här. Inte ens de som har skrivit kan hålla ihop terminologin. Hur ska då dom ska tolka och leva efter det här gör det, när inte ens författarna kan det.

EK: Hur vanligt förekommande är det?

PG: Nja, det är inte så vanligt.

HG: Man kan kanske tänka sig att det bara är ett förslag och att i det man sen antar får man hoppas att de rättar till såna små missar.

PG: Har man inte märkt det nu så... Det är ovanligt. Att man inte ens kan hålla kategorierna. Vi jurister är ju utbilda att se sånt här.

EK: Det säger kanske lite om vilka det är som har lagt fram det.

PG: Ja, det här är ju mycket politiskt. Men att dom inte ens kan hålla, det tycker jag är lite skoj. Då säger dom "Ja, det här blir enkla regler" men ni klarar inte ens själva hålla terminologin, hur enkla är dom då? Fördelen är ju att individens skydd ska stärkas. Det är naturligtvis en signal om att man ska, oavsett hur det här funkar, blir det en signal om att individerna ska skyddas. Det är ju positivt. Svårigheten är då den praktiska tillämpningen. Det behöver man ju inte överdriva. Man kan ju säga "ja, här har individerna och personlig integritet fått ett ökat skydd och det är ju bra". Sen går det inte att i en sån föränderlig värld att skriva såna stela, fasta regler. För verkligheten, då fångar man inte verkligheten. Man måste var så flummig för att fånga verkligheten. Samtidigt blir det svårt att använda den. Så det är mina tankar. Nu är jag inte speciellt insatt i just detta. Jag vet att det är på gång men har inte satt mig in i det. Så är det. Ni frågar nånstans om det blir mer enhetlig tillämpning,,, Ja, det blir det kanske. Sen är det den kulturella anpassningen i olika länder. Det är olika sätt att se på det. Det är det kanske en fördel att det inte blir, för då hämmas företagen. Det är en avvägning hela tiden. Det kanske är en fördel att det är så här löst. Då funkar det och då kan man säga i EU att man har tagit sitt ansvar och skyddar individerna. Vad har hänt då? Jo, vi har ett jättefint regelsystem. Är det många som blir dömda då? Nej, du vet, dom följer reglerna. Det är

mycket politik, detta är ju jättemycket politik.

HG: Finns det någon risk att man siktar för högt? Och det sen inte går att tillämpa?

PG: Ja, det tror jag att man gör men ... alltså man har för stark tro på det här. Det tror jag. Men det gäller alla lagar som är så här tekniska som den här. Man använder om man ser på terminologin, jag skrev ner några ord... Adekvat skyddsnivå, ja, vad är det? Lämpliga skyddsåtgärder. Allmänna principer. Ytterligare precisera. Många undantag är nödvändiga för att.. Man använder såna ord. Ja, vad leder det till? Undantag om överföringen är nödvändig för att kunna och så kommer massa såna "är nödvändigt för att"... Ja, vad betyder nödvändigt? Vems nöd är det? Och så har man undantag från undantag. Men å andra sidan kan man säga att så måste man skriva. Verkligheten är så mångfacetterad kan man inte skriva så stelt. Så det är fascinerande.

EK: Ja, det är en svårbalansgång.

PG: Ja, det är det. Så den har ett stort symbolvärde och det tror jag är positivt. Individernas integritet ska skyddas. Det är en stark symbolik. Det betyder mycket. Man behöver inte raljera alltför mycket. Sen lappar man och lagar och diskuterar.