GDPR i praktiken

Handboken för företag som undrar

Richard Frank

GDPR I Praktiken

En vägledning som riktar sig främst till den som praktiskt ska bedriva arbetet

Richard Frank

ISBN: 978-91-519-3192-0

Förord

Arbetet har utförts hos företaget Infotrust AB. Syftet med detta dokument var att för skapa en bättre förståelse för orsakerna och implementation inom affärssektorn.

Ett stort tack till Christian Hilbertsson som varit ett bollplank under resans gång.
Ett lika stort tack till min hustru som enträget läst dokumentet 100 tals gånger

GDPR I Praktiken

Ansvarig utgivare: Richard Frank
ISBN: 978-91-519-3192-0

Innehåll

 ISBN: 978-91-519-3192-0

1 Sammanfattning

Med den nya dataskyddsförordningen (GDPR) i EU ställs det högre krav på hantering av personuppgifter och för första gången riskerar företag sanktioner om de inte hanterar personuppgifter korrekt, vilket medför att alla organisationer måste ta ställning till hur person-uppgifter skall hanteras inom organisationen. Inom IT-sektorn måste en analys utföras om vilka data som kommer att påverkas med införandet av GDPR och hur data ska hanteras i nuvarande IT-system.

Den nya dataskyddsförordningen och relaterade arbeten har studerats tillsammans med intervjuer som utfördes på olika företag för att framställa ett lösningsförslag. Lösningsförslaget har sedan använts i ett implementeringstest i Infotrust AB s system för att visa att det fungerar. Undersökningen innehåller även en ekonomisk analys för att fastställa betydelsen av att implementeringen hanteras och prioriteras.

Lösningsförslaget som undersökningen tog fram har gett bevisad effekt i systemet och kan med relativ lite resurser återanvändas för att säkerställa att en organisation vidtar tillräckliga åtgärder vid införande av GDPR.

1.1 Nyckelord

Persondata, Integritet, GDPR, Dataskyddsförordningen, Informationshantering

 ISBN: 978-91-519-3192-0

2 Abstract

As a result of the new General Data Protection Regulation (GDPR) in the EU, there are stricter requirements for handling personal data. For the first time, companies risk sanctions if they fail to handle personal data properly, giving rise to a wide spectrum of impacts. In the IT sector, an analysis must be undertaken to determine which data will be affected by the introduction of GDPR and how this data can be managed in current IT systems in order to meet the new requirements. Against this backdrop, this study was conducted at Infotrust AB, a purchasing and electronic trade company located in Malmö.

A proposed solution was developed by studying the GDPR, related works and the results from the interviews which was conducted in this study. The proposed solution was then tested on a selected part of one of the company´s systems. Furthermore, this study presents an economic analysis to determine the significance of implementing of this solution, which points to a need for such a solution to be prioritized by the company.

Overall, the proposed solution proves to have a positive effect with respect to complying with GDPR and can be reused with relatively few resources.

2.1 Keywords

Personal data, Integrity, GDPR, General data protection regulation, Information management

3 Ordlista

Kommers – Kommers annons är en upphandlingsportal som Infotrust AB provat för att hantera bland annat upphandlingar och anbud.

Direktiv - Ett direktiv är en bindande bestämmelse som kräver att de underliggande myndigheterna följer det.

GDPR - General Data Protection Regulation

Förordning - Förordningen hänvisar i denna undersökning till den nya dataskyddsförordningen, även kallad GDPR.

Organisation - I denna undersökning som riktar sig till både företag och organisationer så kommer organisation användas för benämning av båda dessa.

Personuppgifter - Uppgifter som direkt eller indirekt kan identifiera en levande person. I denna undersökning så används personuppgifter istället för personliga data.

Pseudonymisering - ”En teknik som gör det lättare att säkerhetsmässigt hantera personuppgifter. Pseudonymisering innebär att identifierande personuppgifter lagras skilda från övriga personuppgifter. Genom att lagra identifierade personuppgifter från övriga uppgifter, så blir det reglera säkerheten”[1].

(Den) registrerade – Personen som har sina personuppgifter registrerade

Dataportabilitet – Rätten till att få ett utdrag av sina personuppgifter för användande på annat håll till exempel i annan medietjänst.

Fysisk person – En enskild människa och inte en juridisk person.

Big Data – En stor mängd av lagrad digital information att den är svår att bearbeta.

Strukturkapital – Redan investerat kapital i nuvarande organisation. T.ex. redan implementerade tekniska system som hanterar personuppgifter.

ISBN: 978-91-519-3192-0

4 Inledning

Kapitlet inleds med en problemformulering som förklarar vilka problem som organisationer ställs inför med den nya förordningen. Därefter beskrivs målsättningen med undersökningen som följs av avgränsningarna för denna undersökning.

4.1 Problemformulering

Den 25 maj 2018 så kommer den nya dataskyddsförordningen att införas, den nya förordningen ersätter den gamla personuppgiftslagen (PUL) vilket innebär en stor förändring för de flesta organisationer och företag som då måste vara redo för denna förändring. Förändringen kommer inkludera alla IT-system, de olika filerna i filsystemen och dokumenten som ligger på skrivborden som innehåller personuppgifter, med andra ord alla processer där personuppgifter hanteras. Den nya förordningen har tillkommit för att stärka den personliga integriteten för alla privatpersoner i EU. PUL har tolkats olika beroende på vilket land som tolkat den och detta har lett till att hanteringen av personuppgifter skiljer sig mycket beroende på land som gjort tolkningen. Detta är till följd av den enorma tekniska utveckling som skett sedan personuppgiftsdirektivet togs i bruk år 1992. Som det ser ut idag så sparar organisationer personuppgifter genom att användarna godkänner långa användaravtal som ofta är väldigt otydliga, till vilket ändamål och hur personuppgifterna kommer användas är inte tydligt för den registrerade. Det är inte sällan som uppgifterna både lagras osäkert och säljs vidare till andra aktörer på marknaden utan att den registrerade har någon kontroll över det.
Företagen ställs som sagt inför utmaningarna att hantera privatpersoners personuppgifter på rätt sätt enligt förordningen, hur detta ska utföras och vad kostnaden kommer bli ekonomiskt för de berörda företagen för implementering och eventuella sanktioner, det kommer vara de stora frågorna i denna undersökning.

4.2 Målsättning

- Vad är personuppgifter
- Målet är att kunna visa upp detta och om dessa personuppgifter kan delas upp i olika typer eller riskgrupper.
- Ta fram en generell plan för hur data skall hanteras för att möta kraven från förordningen
- Framställa en generell plan på hur en implementation av förordningen kan utföras. Beskriva detta i en process med faser och en förklarande text på vad som ska ske i de olika faserna.
- En generell specifikation för hur en implementation kan utföras
- Att ta fram en checklista som komplement till den generella plan i punkten ovan som sedan kan följas vid implementation av förordningen.
- Visa i en testmiljö att implementeringen fungerar
- Infotrust AB tillhandahåller en testmiljö i deras upphandlingssystem Kommers, i detta testsystem är målsättningen att bevisa att en implementering kan göras i en riktig miljö.
- Undersöka den ekonomiska påverkan som en implementation skapar
- Målsättningen är att göra en analys som visar vad kostnaden för en teknisk implementation som sker i samband med denna undersökning skulle uppgå till. Sedan göra en jämförelse mot att inte implementera dessa förändringar och genom detta utvärdera om den ekonomiska aspekten kan visa vad som är bäst för organisationen att göra.

4.3 Avgränsningar

Att implementera GDPR i hela Infotrust AB s organisation blir för omfattande för denna undersökning. Avgränsningen blir därför att diskutera hur lösningsförslaget som tagits fram i denna undersökning kan anpassas till deras organisation men även att analysera en av deras processer och att implementera tekniska åtgärder för att den processen ska uppnå kraven som medföljer i GDPR. Processen som ska analyseras är ”skapa nytt konto” i systemet Kommers. Avgränsningen gäller även för den ekonomiska analysen som kommer att göras på kostnaden för att implementera de tekniska aspekterna i processen om att skapa nya konton. Den kostnaden kommer att jämföras med vad kostnaden kan bli som följd till att inte vidta tillräckliga åtgärder för att säkra den personliga integriteten för kunderna.

Undersökning är utförd hos en mindre organisation inom koncernen, på grund av detta är lösningsförslaget riktat mot mindre organisationer, vilket inte innebär att lösningen i denna undersökning inte kan användas för myndigheter, sjukhus och företag som ägnar sig åt forskning.

ISBN: 978-91-519-3192-0

5 Bakgrund

GDPR är den nya dataskyddsförordningen som från och med den 25 maj 2018 ersätter den nuvarande Personuppgiftslagen. GDPR är till skillnad från personuppgiftslagen en förordning och inte ett direktiv. En förordning innebär att alla som ingår i den måste följa de nya reglerna och införa dessa på det sättet som anges i förordningen[3]. GDPR införs bland annat för att medlemmarna i EU vill att den fria informationen skall flöda fritt men kontrollerat mellan företag, organisationer och myndigheter men samtidigt skydda den registrerades personliga integritet [1].

Den nya förordningen har arbetats fram tillsammans mellan medlemsländerna för att tillsammans ha en gemensam förordning som kommer se likadan ut i alla länder. Det nuvarande direktivet är inte bara gammalt, det är även enbart ett direktiv vilket har lett till att alla medlemsländer har implementerat det på olika sätt vilket har skapat en stor skillnad i hur personuppgifter behandlas. Personuppgiftslagen togs i bruk 1995 och sedan dess har världen förändrats enormt med teknikframsteg och internets intåg i privatpersoners liv. Detta har gjort att lagen tappat i både kraft och funktion och enligt Colin Tankard så var det så lite som en procent av världens befolkning som använde internet under år 1995 [1]. Denna siffra kan jämföras med siffror från Unstats som säger att 43,75% använde internet år 2015 [4].

ISBN: 978-91-519-3192-0

6 Teori

I detta kapitel presenterar områden som denna undersökning berör utöver den nya dataskyddförordningen. Varje delkapitel innehåller en generell förklaring av ämnet för att skapa en insikt om vad detta innebär för att läsaren ska få en förståelse om detta när det nämns i senare delar av rapporten.

6.1 Arkivlagen

Arkivlagen hanterar bland annat hur länge upphandlingar behöver sparas efter att ett avtal har upphandlats. Om en person begär radering av sina personuppgifter enligt rätten från GDPR så har företaget fortfarande skyldighet att neka denna radering om arkivlagen säger att informationen måste behållas[5].

6.2 Bokföringslagen

Enligt bokföringslagen så måste räkenskaper sparas i sju år efter det kalenderår som räkenskapsåret avslutades[6]. Detta innebär att mycket av de personuppgifter som lagras måste sparas lika länge då dessa uppgifter behövs för att räkenskaperna skall vara kompletta.

6.3 Infotrust AB och Kommers Annons

Infotrust AB utvecklar lösningar inom inköp och elektronisk handel sedan 1998. Med Kommers erbjuds en nyckelfärdig lösning för upphandling, inköp, avtalshantering och e-handel. Kommers Annons är en portal för leverantörer som vill hitta pågående upphandlingar, lämna anbud och hantera e-handel[7].

6.4 Personuppgifter

Datainspektionen har efter innehållet i lagtexten till dataskyddsförordningen definierat personuppgifter på följande sätt ”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt personuppgiftslagen som personuppgifter. Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer”[8]. Datainspektionen har även listat vad som anses vara känsliga personuppgifter enligt dataskyddsförordningen[9]:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Hälsa
- En persons sexualliv eller sexuella läggning
- Genetiska uppgifter och biometriska som entydigt identifierar en person

6.5 JavaScript

JavaScript är ett plattformsoberoende och objektorienterat språk, det används främst för att utveckla webbsidor. JavaScript kan bland annat användas för att skapa iterativa och dynamiskt innehåll till webbsidor som t.ex. växling av annonser eller att dölja visa delar av en webbsida[10].

6.6 Missbruksregeln

I skrivande stund regleras behandling av personuppgifter genom personuppgiftlagen. Personuppgiftslagen skyddar individen från att deras personuppgifter inte används eller sprids utan tillåtelse. I denna lag finns det undantag om hur personuppgifter kan användas för vissa ändamål som publikationer, vilka skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen dvs radio, tidningar tv, film, böcker och webbsidor med en ansvarig utgivare behöver inte tillämpa personuppgiftslagen[11] [12]. Men de måste följa tryckfrihetsförordningen och yttrandefrihetsgrundlagen[13]. Ett annat undantag är missbruksregeln, denna säger

att personuppgifter i ostrukturerad form (i flytande text) får förekomma så länge de inte kränker den personliga integriteten.

6.7 Integritet by design/Privacy by design

Integritetsskydd syftar på principen att endast ta in den information som behövs och inte någonting mer, att inte lagra data längre än nödvändigt och inte använda data till mer än till syftet det samlades in för. Det handlar även om att få samtycke av den registrerade att behandla personuppgifterna för det ändamålet de har inhämtats för och att vara transparent angående hur behandlingen av personuppgifterna kommer att ske.

Privacy by design bygger på principen att lyfta fram integritetsfrågor i början av processen vid utveckling av ett IT-system eller en IT-lösning. Genom att lyfta fram frågan om integritetsskydd tidigt i processen kan man ta hänsyn till de lagar och krav som ställs för att skydda den personliga integriteten och på det viset eliminera risken att hamna i dyra fallgropar, exempel på integritetsfrågor som kan tas upp tidigt och integreras i systemet kan vara[14]:

- Minimera antalet personuppgifter som behandlas
- Åtkomsten till personuppgifter begränsas
- Transparent användargränssnitt för de registrerade kunderna så att det ger den registrerade insyn på hur deras personliga data hanteras
- Skydda personuppgifter från obehöriga

6.8 RSA – Kryptering

RSA-kryptering är en säker och beprövad krypteringsalgoritm som är lätt att förstå och relativt enkel att tillämpa. Den använder sig av en asymmetrisk kryptering, det innebär att den använder en öppen nyckel för att kryptera en text och denna text kan endast dekrypteras med en privat nyckel. Detta gör det möjligt att signera den krypterade texten för att garantera att den dekrypteras av korrekt mottagare[15] [16].

6.9 C#

C# (uttalas C-Sharp) är ett programmeringsspråk som är utvecklat av Microsoft för att köra på .NET ramverket[17] [18]. C# är ett plattformsoberoende programmeringsspråk, det betyder att det kan köras på flera operativsystem. Några olika typer av program utvecklade med C# kan vara konsolprogram, Windowsapplikationer och webbapplikationer.

7 Relaterade arbeten

Några rapporter och artiklar som berör ämnet i denna rapport har studerats för att få ytterligare synvinklar på hur GDPR har tolkats, av andra för att ta fram en generell lösning för hur företagen ska hantera GDPR. Inledningsvis behandlas frågan om vilka utmaningar organisationen ställs inför med införandet av GDPR, det fortsätter sedan med att studera andra synvinklar på hur problemet med borttagandet av missbruksregeln kan hanteras. Kapitlet avslutas med relaterade arbeten på hur företag uppfattar förändringarna, hur dessa förändringar skall ske och vilka förberedelser som krävs för dessa.

Colin Tankar skriver en artikel om GDPR och innebörden av detta för organisationerna [1]. Han skriver om hur GDPR medför striktare regler för organisationen för att skydda den personliga integriteten. Att detta var en nödvändig förändring då den tidigare lagen för att hantera personuppgifter är olika beroende på vilket land som tolkat lagen. Han skriver även att detta ställer högre krav på dataskydd hos organisationerna och ger en kort vägledning på vad organisationerna behöver titta på för att anpassa sig till GDPR. Detta är något som Steve Mansfield-Devine också skriver om i artikeln ”Meeting the needs of GDPR with encryption”, Steve skriver om hur företagen för tänka inför anpassandet till GDPR och möjliga lösningar till detta [2]. Henrik Månsson och Joey Erichsen skriver i rapporten ”Tillmötesgående av GDPR” om vilka de största tekniska utmaningarna företag ställs inför med införandet av GDPR, de skriver även om utmaningarna som tillkommer vid utvecklande av ny teknisk funktionalitet och att implementera detta i nuvarande system [3].

En artikel skriven av Lawrence Ryz och Lauren Grets ”A new era in data protection” är mer fokuserad på hur en person identifieras genom data och vilka undantag det finns för att dela denna data med en tredje-part [4]. Då artikeln är baserad på hur GDPR kommer att påverka e-discovery, skriver de även att hantera data i flytande text kommer bli en tuff uppgift då det inte finns undantag i GDPR för detta[19]. Även Paula Lundholm och Sandra Adolfson skriver i deras fallundersökning ”Detaljhandelns förberedelser inför GDPR” om data i flytande text, de har intervjuat olika företag där de frågat om hur de ska lösa denna fråga [5]. Den visar att det finns stor oro angående data i flytande text och hur de ska lösa detta, endast ett av de intervjuade företagen hade en idé om hur de skall hantera detta. I artikeln ”The GDPR and Big Data: Leading the way for Big Genetic Data?” skriver Kärt Pormeister att risken med att samla in stora mängder personuppgifter identifierats långt innan direktiven med GDPR togs fram. Han skriver även om hur GDPR kommer att påverka Big Data [6].

I en rapport skriven av Maja Brädefors och Julia Petterson undersöker de frågan ”Hur uppfattar företag de förändringar som GDPR innebär och hur går de tillväga med förberedelserna inför den nya lagen?” [7]. De skriver om vad GDPR innebär och hur förändringsprocesser kan se ut hos företag. De har även intervjuat företag angående detta, analyserat och jämfört deras svar för att se hur de olika företagen löser frågan om GDPR. Det skrivs även om förberedelser inför GDPR i artikeln ”The Year of the GDPR” skriven av Kim Smouter, i den artikeln nämner Kim tre viktiga steg som bör tas i beaktande vid anpassning till GDPR och kompletterar detta med en checklista för anpassning till GDPR [8] [9].

Ytterligare en åtgärd det talas om väldigt mycket är privacy by design, att lyfta fram frågan om integritetsskydd tidigt i processen. Detta är något som Harald Gjermundrod, Ioanna Dionysiou och Kyriakos Costa skriver om i en artikel där de även skriver att det inte finns ett tydligt ramverk för att implementera detta [10].

8 Analys av dataskyddsförordningen

En undersökning på Dataskyddsförordningen i sin helhet, undersökningen har delats upp i kapitel i samma ordning som förordningstexten är uppdelad. De delar ur GDPR som anses vara viktigast för projektet visas här upp och förklaras. Referenserna är till länkade delar ur förordningen men specifika kapitel och artiklar kommer nämnas vid behov [11].

8.1 Allmänna bestämmelser

Detta kapitel i GDPR förklarar översiktligt hur förordningen är tänkt att användas och hur den skall användas beroende på vilken typ av person, företag eller organisation som frågan berör. Artikel 1 säger att förordningen avser att fastställa bestämmelser för hur behandling av personuppgifter skall utföras samt hur det fria flödet av personuppgifter skall ske. Förordningens första kapitel, artikel 1 säger bl.a. detta, "Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter"[20]. Resterande delar av förordningen förklarar tillämpningsområden och definitioner.

Slutsats: Förklarar hur förordningen skall användas av berörda aktörer och till vilket ändamål den har införts.

8.2 Principer

Personuppgifter som samlas in för särskilda ändamål skall behandlas på ett lagligt, korrekt och öppet sätt gentemot den registrerade det gäller och det uttryckligt angivna ändamålet. Det är de fastställda ändamålen som sätter ramarna för behandling av personuppgifterna. Om personuppgifterna vidare ska behandlas för arkivändamål som uppfyller arkivlagen eller bokföringslagen är det då detta som gäller för arkivering av personuppgifter[21]

[22.] Personuppgifterna som inhämtas ska vara uppdaterade, relevanta och överensstämma med ändamålet de ska behandlas för. För att säkerställa att uppgifterna är korrekta ska rimliga åtgärder användas för att säkerställa att de inte är felaktiga. Den registrerades uppgifter ska förvaras så att den registrerade inte kan identifieras under en längre tid än nödvändigt för det ändamålet personuppgifterna behandlas.

Personuppgifterna ska behandlas på ett säkert sätt som skyddar mot otillåten behandling, obehöriga, förlust, förstöring eller skada genom olyckshändelse. Detta skall hanteras genom att använda lämpliga tekniska eller organisatoriska åtgärder. För att behandling av personuppgifter ska vara lagligt måste personen som detta berör lämna sitt samtycke och att den registrerades personuppgifter behandlas enligt ett eller flera specifika ändamål.

Behandlingen kan enligt förordningen vara nödvändig för om:

- Parterna ska ingå i ett avtal eller utföra vissa åtgärder på begäran av personen i frågan innan ett avtal ingås.
- Fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (ska fastställas i enlighet med unionsrätten eller en medlemsstats nationellas rätt som den personuppgiftsansvarige omfattas av).
- Skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- Utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (ska fastställas i enlighet med unionsrätten eller en medlemsstats nationellas rätt som den personuppgiftsansvarige omfattas av).
- Ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Vid inhämtning av personuppgifter för informationssamhällets tjänster direkt till ett barn som är under 16 år ska samtycket godkännas av en person som har föräldraansvar för barnet. Personuppgiftsansvariga måste kontrollera att samtycket godkänns av personen med föräldraansvar för barnet.

Om personuppgifter behandlas för andra ändamål än det särskilda ändamålet de samlades in för som utgör en nödvändig och proportionell åtgärd för att skydda de mål som avses i artikel 23.1. Personuppgiftsansvariga ska

bevisa hur behandlingen för andra ändamål är överensstämmande med de ändamålen personuppgifterna samlades in.

- De ska betrakta kopplingar mellan de ändamålen personuppgifterna har samlats in och ändamålen de ytterligare använts för.
- Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.
- Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter
- om fällande domar i brottmål och överträdelser behandlas i enlighet med artikel 10.
- Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.
- Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Personuppgiftsansvariga ska kunna visa att personuppgifterna som har samlats in grundar sig på samtycket, att personen har samtyckt till behandling av personuppgifter. Om samtycket lämnas i en skriftlig förklaring ska samtycket förklaras på ett tydligt och begripligt sätt med användning av klart och tydligt språk. Personen ska på egen begäran när som helst kunna återkalla sitt samtycke. Detta påverkar inte behandling som redan har utförts under samtycket av personen.

Att behandla personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter, biotermiska uppgifter för att identifiera en fysisk person, uppgifter om hälsa eller om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden om inte samtycke till behandling av dessa uppgifter har lämnats[23].

Slutsats: Personuppgifter får enbart samlas in när behov för detta finns och samtycke har inhämtats från den registrerade för att skydda den personliga integriteten. Det är den insamlande aktörens skyldighet att behandla uppgifterna lagligt, korrekt och öppet i förhållande till den registrerade.

8.3 Den registrerades rättigheter

Den registrerades rättigheter har ökat med införandet av GDPR. Den största delen är att den fysiska personen måste informeras på ett enkelt och lättförstått sätt om hur de olika personuppgifterna sparas, varför, hur länge dessa skall sparas, vem som är ansvarig över hanteringen av personuppgifterna och vad den registrerade har för möjligheter och rättigheter i hanteringen av de erlagda personuppgifterna. Den registrerade har även rätten att få tillgång till personuppgifterna organisationen har om den registrerade, rättelse och radering, rätten till att begränsa behandlingen av personuppgifterna och rätt till dataportabilitet. Det finns utöver dessa rättigheter flera tillägg om hur den fysiska personens uppgifter skall hanteras och i vilka fall dessa är tillämpbara[24] [25] [26] [27] [28].

Slutsats: Den datainsamlande aktören måste på ett tydligt och enkelt sätt förvisa sig om att den registrerade vet hur och varför personuppgifterna sparas. Den registrerade måste även få reda vilka möjligheter den har för hanteringen av personuppgifterna.

8.4 Personuppgiftsansvarig och personuppgiftsbiträde

En personuppgiftsansvarig är enligt förordningen “en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter”[29]. Den personuppgiftsansvarige är ansvarig för att alla personuppgifter hanteras enligt den förordningen som finns. Den ansvarar för att de tekniska och organisatoriska förändringar som krävs och att organisationen och de anställda förstår vikten av att hanteringen görs på det sätt som har beslutats av den personuppgiftsansvarige. Den personuppgiftsansvarige är också ansvarig för att detta följs fortsättningsvis och uppdateras vid behov. För att den personuppgiftsansvarige skall kunna visa på att den fullfört sina uppgifter så finns det enligt artikel 40 och 42 olika uppförandekoder och certifieringsmekanismer som får användas för att visa på att man efterlever de gällande reglerna.

Om organisationen uppnår något av dessa krav så är det den personuppgiftsansvarige som är skyldig att införa ett register över vilka personuppgiftsbehandlingar som utförs:

- Företaget har mer än 250 anställda
- Finns risk för den registrerades rättigheter och friheter
- Att behandlingen inte är tillfällig.

Personuppgiftsbiträdet är en fysisk eller juridisk person som är utsedd av den personuppgiftsansvarige att hantera den personuppgiftsansvariges data enligt de givna riktlinjerna. Detta skall regleras i avtal och vara väl specificerat. Ett personuppgiftsbiträde måste för att kunna bli utsedd kunna garantera den tekniska och organisatoriska säkerheten som krävs för den typen av personuppgifter som skall hanteras[30].

Dataskyddsombud utses av personuppgiftsansvarige och personuppgiftsbiträdet om någon av dessa tre frågor stämmer in hos organisationen[31]:

1. Är ni en myndighet eller en folkvald församling, det vill säga ett offentligt organ?
2. Har ni som kärnverksamhet att regelbundet, systematiskt och i stor omfattning övervaka enskilda personer?
3. Har ni som kärnverksamhet att behandla känsliga personuppgifter eller uppgifter om brott i stor omfattning?

Dataskyddsombudets uppgifter är att övervaka att dataskyddsförordningen följs i sin helhet hos organisationen. Att finnas tillgänglig för personuppgiftsansvarige och personuppgiftsbiträde för att ge råd gällande konsekvensbedömning av dataskydd. Dataskyddsombudet samarbetar med tillsynsmyndigheten och agerar som kontakt när tillsynsmyndigheten behöver information från organisationen.

Slutsats: Den personuppgiftsansvarige är skyldig att bevisa att förordningen följs även om den tecknat avtal med ett personuppgiftsbiträde som sköter den faktiska hanteringen av personuppgifter. För att kunna redogöra för den registrerade vilka personuppgifter som behandlas och syftet med behandlingen samt att dessa är säkrade för intrång. Ett personuppgiftsbiträde hanterar den personuppgiftsansvariges data enligt förordningen och avtalet mellan de två parterna. Personuppgiftsombudet vid de tillfällen en sådan krävs övervakar att organisationen följer förordningen och agerar som en kommunikationslänk mellan datainspektionen och den personuppgifts-ansvarige eller personuppgiftsbiträdet

8.5 Överföring av personuppgifter till tredjeländer eller internationella organisationer

För att personuppgifter får överföras till ett tredjeland eller en internationell organisation måste EU-kommissionen beslutat att de i frågan har säkerställt likvärdig skyddsnivå och överföringen ska då inte kräva något särskilt tillstånd[32]. Kommissionen ska även övervaka utvecklingen i tredjeländer och internationella organisationer vilket kan påverka tidigare tagna beslut. Under följande situationer får överföring av personuppgifter till tredjeland eller internationella organisationer ske med förutsättningarna att reglerna i förordningen följs.

- Lämpliga skyddsåtgärder
- Särskilt tillstånd av Datainspektionen
- Samtycke eller i andra särskilt angivna situationer
- Överföring vid enstaka tillfällen

Slutsats: För överföring av personuppgifter till tredjepartsland behöver samtycke inte inhämtas om det är likvärdig skyddsnivå eller kraven för något av de fyra undantagen ovan uppfylls.

8.6 Oberoende tillsynsmyndigheter

Varje medlemsstat skall utnämna en eller flera oberoende myndigheter som ska ansvara för tillämpningen av förordningen för att skydda den enskilda personens rättigheter genom att övervaka de som behandlar

personuppgifterna och att de gör detta enligt dataskyddsförordningen. Tillsynsmyndigheten ska förmedla risker, regler, skyddsåtgärder och rättigheter om hur behandling ska gå till. De ska även varna och beordra organisationer att ta till åtgärder vid behandling av personuppgifter, de kan även begränsa eller förbjuda behandling av persondata hos organisationer samt att besluta om sanktionsavgifter. Tillsynsmyndigheten kan även förse den enskilda personen med information om deras rättigheter med anledning av förordningen.

Slutsats: Varje medlemsstat måste utse en eller flera myndigheter som är skyldiga att upprätthålla förordningen genom att förmedla förordningen och övervaka att den följs.

8.7 Samarbete och enhetlighet

Med samarbete så menas de flesta typer av samarbete men framförallt handlar det om att tillsynsmyndigheten ska samarbeta tillsammans med andra länders tillsynsmyndigheter på ett snabbt och smidigt sätt och med de organisationer eller personer som har någon form av kontakt med tillsynsmyndigheten. Tillsynsmyndigheten måste bistå med kommunikation mellan de olika ländernas tillsynsmyndigheter och de skall även kommunicera med de organisationer eller personer som har åsikter om hantering av personuppgifter.

Slutsats: Tillsynsmyndigheten är skyldig att hantera kommunikation mellan tillsynsmyndigheter och organisationer eller personer, de skall agera som en mellanhand.

8.8 Rättsmedel, ansvar och sanktioner

Enligt kapitel VIII, Artikel 77 så har alla fysiska eller juridiska personer som anser att dennes personuppgifter har behandlats på felaktigt sätt rätt att lämna in ett klagomål till tillsynsmyndigheten som är ansvarig för den medlemsstat där klagomålet gäller, oftast är det den tillsynsmyndighet som finns i personens hemland. Kommunikation mellan tillsynsmyndigheten och personen i frågan angående det pågående ärendet skall skötas av tillsynsmyndigheten om hur ärendet fortskrider. Tillsynsmyndighets ansvarar för vilken typ av sanktion som en personuppgiftsansvarig eller ett personuppgiftsbiträde kan åläggas beroende på vilken typ av överträdelse som har skett. Detta framförallt enligt artikel 83 tillsammans med artikel 58.2. Sanktionerna kan röra sig mellan varningar i förväg om att en överträdelse mot förordningen förmodligen kommer ske med tanke på någon form av förändring, till sanktioner på upp till 20 000 000 € eller 4% av den globala årsomsättningen. Det finns både lägre sanktionsavgifter och enbart reprimander i straffskalan. Det beror helt på överträdelsens art, hur stor den är, vad för åtgärder som gjorts i förväg för att förhindra det och flera andra värderingar kan göras enligt förordningens artikel 83, både försvårande och förmildrande.

En person som på något sätt har lidit skada på grund av en organisations hantering har enligt Artikel 82 rätt till ersättning beroende på situation och händelse, detta från den personuppgiftsansvarige eller personuppgiftsbiträdet alternativt båda två.

Slutsats: Tillsynsmyndigheten har skyldighet att se till att inrapporterade klagomål hanteras och kontrolleras. Om felaktigheter i behandlingen skett från den personuppgiftsansvarige så skall tillsynsmyndigheten bestraffa denne enligt förordningen.

8.9 Bestämmelser om särskilda behandlingssituationer

Vissa situationer kräver särskild behandling av personuppgifter för utförande av vissa ändamål, medlemsstaterna ska ta fram särskilda bestämmelser dvs undantag eller avvikelser beroende på situation. Dessa behandlingssituationer har delats upp i följande områden och de har egna specifika undantag som måste uppnås för behandling av personuppgifter[33].

- Yttrande- och informationsfriheten
- Allmänhetens tillgång till allmänna handlingar
- Nationella identifikationsnummer
- Anställningsförhållanden
- Skyddsåtgärder och undantag för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål
- Tystnadsplikt
- Befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund

Slutsats: Förordningen har vissa undantag då det finns lagar som är starkare, dessa undantag är oerhört viktiga att hantera och kontrollera.

8.10 Delegerade akter och genomförandetakter

Rättigheten att ta emot delegerade akter som avses i artikel 12.8 och 43.8 ska lämnas till kommissionen från och med den 24 maj 2016. När kommissionen mottar en delegerad akt ska de informera Europaparlamentet och rådet. Den befogenheten kan även återkallas av Europaparlamentet eller rådet det innebär att befogenheten slutar gälla dagen efter detta offentliggjorts i Europeiska unionens officiella tidning eller vid ett givet datum.

9 Metod

I detta kapitel beskrivs de olika stegen i undersökningen för att ge en djupare förklaring för hur arbetet har fortskridit och vilka metoder som har använts genom undersökningen. Kapitlet börjar med att förklara vilken typ av metod som har valts till undersökningen för att sedan fortsätta och beskriva intervjumetoden och avslutningsvis beskriva genomförandet av den tekniska implementationen i undersökningen.

9.1 Strategi för undersökningen

Den valda metoden för den här undersökningen är en kvalitativ fallundersökning som Alan Bryman skriver om i Social Research Methods [12]. Denna metod använder sig av flera datainsamlingsmetoder som intervjuer, observationer och dokumentanalys för att samla in data som ska analyseras för att få en djup förståelse för ämnet i undersökningen. Utifrån detta valdes intervjuer, litteraturundersökningar och att deltaga i seminarier som metoder att samla in data till denna undersökning. Metoderna för att samla in data valdes då den största källan för denna undersökning är Datainspektionen och förordningstexten för den nya dataskyddsförordningen. När den nya förordningen och olika tolkningar av den analyserats noggrant togs ett lösningsförslag fram som resultat av undersökningen. Därefter intervjuades två olika organisationer för att sedan jämföra lösningsförslaget med resultatet från intervjuerna som var baserad på hur andra organisationer har löst samma fråga hos dem. Slutligen implementerades en del av lösningen i Kommers system vilket visas i kapitel 8 och diskuteras i kapitel 9.

9.2 Intervjuer

Intervjuerna var menade för att använda som forskningsmaterial i undersökningen och att jämföra lösningar hos andra organisationer med resultatet i denna undersökning. Det var då viktigt att få en djup förståelse för hur andra organisationer har tolkat GDPR och vilka lösningar de har för att implementera det i organisationen [13]. Den valda intervjumetoden till denna undersökning blev då en semistrukturerad intervjumetodik som går ut på att förberedda frågor inför intervjun och följdfrågor anpassas beroende på vilket svar den intervjuade ger. Genom att använda en semistrukturerad teknik öppnar det för att intervjun ska bli ett mer naturligt samtal och följdfrågorna som är anpassade till svaret som ges ger ett mer djupgående svar på den ursprungliga frågan som ställts. Detta ger en viss struktur för att inte hamna i fel riktning på intervjun samtidigt som den intervjuade får möjlighet att tala fritt runt frågorna som ställs.

9.3 Tekniskt genomförande

Processen i Kommers som undersökningen behandlar analyserades noggrant och en modell på denna process skapades tillsammans med Infotrust AB. Detta gjordes för att skapa en förståelse för vad som sker i processen och hur personuppgifter hanteras i organisationen och i systemet. Därefter diskuterades alternativa lösningar för hur GDPR kan implementeras i denna process för att sedan när ett beslut togs angående en lösning så implementerades denna i systemet.

9.4 Ekonomisk analys

Kostnadskalkylering för implementationen och en kostnadskalkylering där en implementation inte gjorts. En jämförelseanalys har gjorts på dessa två kostnadskalkyler. Tabeller har skapats för att kunna visa upp ett resultat som senare fritt har diskuterats beroende på vilka scenarion som har kunnat förutspås via en workshop tillsammans med Infotrust AB.

En jämförelse av denna kostnadskalkylering har utförts med ett företag, hädanefter kallat företag X som är betydligt mer etablerat på marknaden och större i antalet anställda. Kostnadskalkyleringen som användas från företag X är inte på hela implementationen av GDPR på företaget utan den är avgränsad till en liknande implementering som denna rapport hanterar. Företag X har flera projekt igång parallellt och kostnaderna för dessa projekt är väldigt lika.

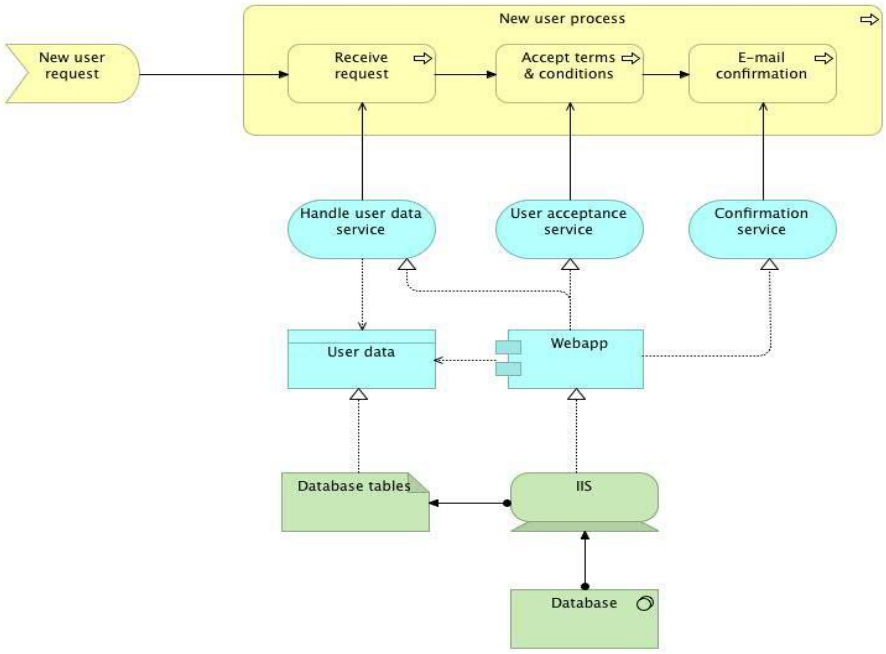
En intervju med företag Y har också utförts där en jämförelse var svårare att göra då de hade tagit ett större grepp och inte delat upp det i lika små system. Företag Y pratade mer om att kostnaden för GDPR är oerhört individuell då det redan investerade strukturkapitalet skiljer sig väldigt mellan företag. Ett företag som hanterat personuppgiftslagen på ett bra sätt har enligt företag Y redan väldigt mycket av administrationen och det mesta i systemen klart för GDPR. Detta medför en lägre kostnad för införandet av förändringarna för GDPR. Detta ger en svårighet i att jämföra de olika företagens kostnader.

10 Leverantörsregistrering i Kommers

Detta kapitel förklarar den processen i Kommers som denna undersökning analyserar. Den beskriver hur en registrering av ett leverantörskonto i Kommers går till innan implementeringen av GDPR har genomförts.

Registrering

När en leverantör vill ansluta sig till Kommers så använder de sig av en registreringsfunktion på hemsidan. Denna funktion illustreras nedan i figur 7.1 och bilaga B visar hur det ser ut i systemet. En användare kommer in på hemsidan och väljer att starta en registreringsprocess. De tre olika stegen i processen är ”Receive request” här anger användaren sina uppgifter och klickar sedan registrera. Nästa steg är ”Accept terms & conditions” som kontrollerar att användaren har godkänt gällande avtal vilket är ett krav för att användaren ska få registrera sig. När detta steg är klart lagras den registrerades person-uppgifter i databasen se Bilaga C, här visas det att endast lösenordet är krypterat i databasen. Det tredje och sista steget i processen är ”E-mail confirmation” som hanterar ett aktiveringsmail som användaren måste godkänna, detta steg utförs för att kontrollera att det är rätt person som försöker skapa användarkontot.



Figur 7.1 - Visar processen över hur en ny leverantör registrerar sig i Kommers och får tillgång till ett användarkonto.

11 Resultat

I detta kapitel redovisas resultatet av undersökningen, kapitlet svarar på de frågor som presenterades i målsättningen och resultatet av intervjuerna som utfördes för denna undersökning. Kapitlet är indelat i underkapitel och börjar med att redovisa definitionen av personuppgifter för att sedan presentera resultatet av intervjuerna. Kapitlet fortsätter sedan för att presentera den generella plan som framställts av denna undersökning och vilka resultat som framkommit genom användning av denna generella plan i en avgränsad del i systemet Kommers. Kapitlet avslutas med att presentera de ekonomiska aspekterna för användning av den generella planen och implementationen av de tekniska delar i Kommers som denna undersökning behandlade.

11.1 Definition av personuppgifter

Tidigare i rapporten beskrivs personuppgifter under rubrik 3.4 där datainspektionen har tolkat dataskyddsförordningen och beskriver vad som anses vara personuppgifter och vad som anses vara känsliga personuppgifter enligt förordningen. Detta anses som en god och tydlig beskrivning av vad personuppgifter är som senare analyseras och diskuteras ur ett GDPR perspektiv under diskussion i rapporten.

11.2 Intervjuer

Intervjuerna gjordes enligt metoden i kapitel 6 vilket skapat lite olika svar från intervjuobjekten som kommer benämnas som företag A och företag B. Företag A är ett väldigt litet företag med få anställda, företag B är precis tvärtom, ett stort företag. Båda företagen hanterar mycket personuppgifter i sin verksamhet.

11.2.1 Utbildning, medvetenhet, personuppgiftsidentifiering och samtycke

För att skapa medvetenhet om GDPR så har båda företagen utbildat sin personal, dock på lite olika sätt, företag A har använt sig av Datainspektionens utbildningar där hela företaget deltagit, företag B har tagit in konsulthjälp för att hantera övergången och har själva en egen complianceavdelning som hanterar utbildningen för de anställda[34]. Denna avdelning väljer vilka som får vilken typ av utbildning och de sätter ihop det arbetssätt som skall användas, allt för att se till att arbetet går till på samma sätt oberoende av om det är flera personer som gör samma arbete. I företag B har man då också kommit fram till att fler typer av roller kommer att behövas i deras CRM-system för att hindra personuppgiftsincidenter.

Företag A har efter utbildningen tagit fram vilken typ av personuppgifter de behandlar, senare har de gjort en indelning i vilken klassning den identifierade data skall ges, de anger att de inte har någon direkt form av extern ostrukturerade data då de själva hanterar sin kunddata i en databas och inte i filer men att de har en del interna ostrukturerade data. Då Företag B mestadels redan har kontroll över exakt vilka personuppgifter de hanterar då anses inte denna del vara ett problem, den utmaning de har istället är att hantera den ostrukturerade data som de har i en gemensam fil-yta som vid detta tillfälle är på cirka fem miljoner filer som är helt okontrollerade. De tänker hantera detta genom att sätta läsrättigheter på hela fil-ytan för alla anställda som måste gå igenom fil-ytan och hämta ut de filer som den anställda anser sig behöva. Detta skall ske innan ett specifikt datum som infaller före den 25 maj. De filer som den anställda får spara för att utföra sitt arbete enligt företagets styrdokument måste placeras på rätt plats som finns anvisad. Sedan kommer hela fil-ytan att låsas för alla förutom en chefsgrupp som kan ge tillgång ifall någon saknar någonting. Denna fil-yta kommer sen ligga låst under en förutbestämd tid innan den helt raderas då det kan anses vara information som är utdaterad. Företaget vet inte om detta är en godkänd metod enligt förordningen men de anser att det är försvarbart att hantera det på detta sätt. Båda företagen diskuterade samtycke och hade lite olika tankar om detta. Företag A behöver hantera samtyckte både för personer äldre än 13 men även yngre, detta skapar ett behov av att kunna identifiera både vårdnadshavare och personen som skall registreras. Företag A ser detta som ett ganska stort problem då det både är dyrt och svårt att identifiera vem det är som samtycker till deras registrering för marknadsföring. Företag B vill bemöta detta genom att undvika samtycke så långt som möjligt då det kan dras tillbaka från den registrerade närsomhelst. De vill att kunderna ingår avtal om de tjänster de tillhandahåller så att företaget kan anse sig behöva personuppgifterna för att kunna utföra sina arbetsuppgifter för kunden. De säger att sådana avtal inte går att bryta på samma sätt då det finns andra lagar som kräver att hanteringen av den registrerades personuppgifter sparas för t.ex. bokföring.

11.2.2 Risker, incidenthantering och backup

Hanteringen av risker och incidenter har hanterats på lite olika sätt av de två företagen, Företag A har sett att den största risken är att de skulle kunna bli överösta med förfrågningar om registerutdrag då de är i en bransch där deras kunders användare kan tänkas vilja veta detta. Då företaget är litet kan detta ta upp mycket av deras resurser om inte en automatisk funktion för detta skapas. Företag B har i sin tur enbart haft en enda förfrågan om registerutdrag på en period av sju år. De anser att de inte behöver förbereda sig för ett sådant scenario med en automatisk funktion utan de väljer att enbart skapa ett styrdokument för manuell hantering. Företag A har även identifierat en risk angående deras lagring av data, deras databas och webbserver ligger på samma server. Med andra ord, om de skulle vara med om ett intrång i servern kommer angriparna åt både webbapplikationen och hela databasen. Detta har gjort att företag A inte krypterar någonting mer än lösenorden för användarna då ett intrång ger tillgång till dekrypteringsnycklarna för databasen också. Företag B anser att de inte har några förhöjda risker angående datasäkerheten med den nya förordningen då de sedan tidigare har höga krav på säkerhet i sina system.

Framförallt företag A diskuterade backuper som både en risk och ett problem då det inte finns tydliga riktlinjer för hur backuper och framförallt gallring i backuper skall hanteras. De säger att rent tekniskt är det ett enormt arbete att ta bort specifika saker ur en backup vid en radering. De anser själva att det borde räcka med att alla backuper tas bort med jämna mellanrum och att informera om detta när den registrerades personuppgifter inhämtas. Företag B hade inga åsikter om detta.

11.3 Generell plan för implementation av GDPR

Genom att analysera GDPR i sin helhet har en generell rekommendation tagits fram i form av ett lösningsförslag som har delats upp i tre faser: förundersökning, riskanalys och innehåll i implementering (se figur 8.1), dessa följs av en checklista på vad en organisation bör ta i beaktande för att implementera GDPR.

Figur 8.1 - Illustration av Fasindelning

11.3.1 Fas I - Förundersökning

En utförlig förundersökning bör genomföras för att läsa in sig om GDPR är och förstå hur organisationen måste förhålla sig till kraven i dataskyddsförordningen. Genom att göra detta skapas en kunskap som sedan kommer att användas för att identifiera delar i organisationen där behandling av personuppgifter behöver hanteras. Det är viktigt att det inte är enbart en person eller en liten grupp som lär sig om vad förordningen säger utan att informationen även förs vidare till hela företaget.

11.3.2 Funktioner och processer

Identifiera vilka processer i organisationen som hanterar personuppgifter, analysera sedan dessa processer för att bedöma om åtgärder måste vidtas för att uppnå kraven i förordningen. Att även ta reda på om dessa processer skickar data till tredje part för behandling är väldigt centralt för att skydda den personliga integriteten. Att även identifiera alla säkerhetsåtgärder som finns i dessa processer är centralt för att kunna göra en bra riskanalys.

11.3.3 Personuppgifter

Kartlägga och skapa ett register över alla personuppgifter organisationen behandlar och dela upp dessa i direkt och indirekt identifierande data. Här ska även data som behandlas i ostrukturerad form identifieras dvs om organisationen använder sig av missbruksregeln. Detta underlättar vid senare tillfälle då även en riskanalys av dessa personuppgifter skall utföras. Då personuppgiftsansvarig måste överlämna ett register av den personuppgiftsbehandling som görs i organisationen till datainspektionen är detta ett bra stöd för att skapa registret vid ett senare steg. Personuppgifter är all slags data som kan relateras till en levande fysisk person. Exempel på personuppgifter kan vara namn, e-postadress, ljudinspelning, bilder, IP-adress. Hur denna data inhämtas ska också identifieras för att analysera vad den registrerade får för information och hur den lagras, insamling av data kan exempelvis ske på följande sätt formulär (online/offline), offerter, mailkorrespondens och hälsodata genom stegräknare.

Vilka personer i organisationen som hanterar personuppgifter bör också identifieras då dessa måste informeras om vad som gäller med den nya förordningen för att hantera personuppgifter på ett korrekt sätt. Detta steg är också viktigt då alla personer inte ska ha tillgång till personuppgifter som behandlas.

11.3.4 Samtycke

Hur ni i dagsläget inhämtar samtycke för behandling av personuppgifter ska också analyseras då detta är en viktig punkt i den nya förordningen. Hur är användarvillkoren strukturerade, är det juridisk text eller är det lättförstått även för någon utan denna kunskap? Hur tydligt är det för den som registrerar sig angående hur och varför lagring sker men även till vilket ändamål sker inhämtning av personuppgifter?

11.3.5 FAS II – Riskanalys

En riskanalys måste utföras för att ta fram vilka risker som både företaget står inför med den nya förordningen och vilka risker företagets kunder står inför. Riskanalysen måste utföras direkt efter förundersökningen då företaget har som mest kontroll över vilka personuppgifter de hanterar. Hur kan företaget påverkas om förordningen inte följs. Även om Checklistan i Bilaga A inte är specifik för ett företag ger den en bra bild av vilken typ av frågor som måste ställas.

11.3.6 FAS III – Innehåll i implementering

För att implementera allt innehåll så behöver den personuppgiftsansvariga organisationen utse en ansvarig som sätter ihop ett kompetent team som hanterar implementeringen och tillsammans med denna sammanställa en tidsplan. Denna grupp måste sammanställa vad som behöver hanteras, genom att använda sig av Fas I och II tillsammans med rekommendationerna i Fas III då kommer hela innehållet kunna hantera företagets övergång till att vara GDPR-Ready.

11.3.7 Utse dataskyddsombud

Ett personuppgiftsombud är den personen som skall överse att den personuppgiftsansvarige hanterar personuppgifter enligt de föreskrifter som har tagits fram. Ett personuppgiftsombud bör inte vara en person i nyckelposition då personuppgiftsombudets omdöme kan ifrågasättas. Förordningen har en del riktlinjer som är till för att hjälpa till i denna procedur, se kapitel 5.4.

11.3.8 Utse personuppgiftsbiträde

Ett Personuppgiftsbiträde kan utses men kommer förmodligen att bli identifierat. Då många företag har outsourcat hela sin datahantering till ett datacenter fungerar då detta datacenter som ett personuppgiftsbiträde. Här är det viktigt för den personuppgiftsansvarige att ta fram tydliga avtal med raka krav på hur personuppgiftsbiträdet skall hantera och säkra de personuppgifterna som lagras, detta beskrivs i kapitel 5.4.

Företaget själv kan vara både personuppgiftsansvarig och personuppgiftsbiträde det är då viktigt att analysera om det finns någon kund där företaget fungerar som personuppgiftsbiträde och dessa avtal måste också hanteras, på det sättet som ovan. Om företaget har många kunder där personuppgifter lagras är det viktigt att erbjuda en bra tjänst med bra hantering av den nya förordningen för att försöka få alla avtal med kunderna att vara lika varandra.

11.3.9 Nya rutiner för dataskydd

De processer som identifierats i FAS I som inte uppfyller de tekniska säkerhetsåtgärderna för dataskydd ska uppdateras/ändras till att de uppfyller de kraven som ställs för tekniskt dataskydd i GDPR. Nya rutiner för dataskydd eller begränsningar av systembehörigheter kan vara alternativ för detta.

11.3.10 Dokument som måste framställas/uppdateras

Rättsliga dokument: Att utforma de nya avtalen gällande hanteringen av personuppgifter både mellan den egna organisationen och deras personuppgiftsbiträde är av oerhörd vikt. Dessa avtal skall vara GDPR säkrade. Om du som organisation har flera personuppgiftsbiträden är det viktigt att man tar fram ett avtal som används till samtliga personuppgiftsbiträden för att försäkra sig om att datahanteringen sker enligt organisationens tolkning av GDPR.

Samtycke från kund/användare: Enligt GDPR:s specifikationer uppdatera informationen som ges till kunden vid inhämtning av data, ge dem information angående hur deras personuppgifter kommer att behandlas och till vilket ändamål denna data inhämtas. Att utveckla en standardtext som kan användas vid flera situationer är en bra lösning för detta.

Fastställa rutiner för uppföljning av implementation av GDPR: Det ska övervakas att reglerna från GDPR följs och otillräckliga åtgärder eller vid brister ska detta rapporteras. Att fastställa rutiner om hur detta ska övervakas och rapporteras ska göras för uppföljning av efterlevnaden av GDPR.

Styrdokument: Fastställa rutiner i form av styrdokument på hur personal ska agera vid olika scenarier som tillkommer med GDPR, dessa olika scenarier förklaras mer noggrant i kapitel 5.3:

11.3.11 Begäran av registerutdrag

- Hur personal ska agera vid incidenter eller misstanke om incident har identifierats
- Hantering av persondata för de i organisationen som behandlar personuppgifter
- Begäran om radering, ändring och begränsning av personuppgifter som är registrerad
- Rutiner för dataportabilitet

11.3.12 Utbildning

Medarbetarna i organisationen som behandlar personuppgifter behöver kunskap inom GDPR för att hantera personuppgifter på ett korrekt sätt, att säkerställa att rätt personer har rätt utbildning är den personuppgiftsansvariges ansvar[35]. Vissa roller kan även behöva fördjupad kunskap, t.ex. dataskyddsombudet, avdelningschefer, IT-avdelningen eller HR.

11.3.13 Raderingsrutiner

Fastställa anvisningar angående företagets egna raderingsrutiner. Hur länge och till vilket ändamål behöver data lagras efter avslutat ärende där ärendet innebär behandling av personuppgifter. Detta ska fastställas och införas i samtycket som kunden godkänner då organisationen inhämtar personuppgifter i första steget som framstår i kapitel 5.2.

11.3.14 Transparens mot kund (skapa ett transparent användargränssnitt)

Med den nya förordningen är det ett krav att man skall vara transparent mot den registrerade, detta kan lösas på flera sätt såsom styrdokument och liknande. Om man som organisation har ett användargränssnitt där den registrerade kan logga in, då är det möjligt att skapa en funktion på t.ex. "mina sidor" där organisationen fortlöpande visar vilka personuppgifter de har om den registrerade användaren.

11.4 Checklista för implementering

Tabell 8.1 nedan är ett utdrag ur checklistan som finns i sin helhet i bilaga A. Den har utarbetats genom information och punkter från Datainspektion tillsammans med denna undersöknings tolkningar och jämförelser från de intervjuer som utförts hos företag A och B. I tabellen förklarar den vänstra kolumnen vilka som har delaktighet i varje punkt.

Tabell 8.1 - S = Undersökningen, D = Datainspektionen.

Fas I - Förundersökning		Resultat av analys
S	Läsa in om vad GDPR är och förstå hur ni måste förhålla er till kraven i dataskyddsförordningen.	
S	Vilka funktioner och var hanterar ni personliga data (processer)	
S	Interna processer som behandlar personuppgifter	
D	Tredje parts behandling av personuppgifter	

11.5 Implementering av lösningsförslag i Kommers

11.5.1 Fas I – Förundersökning

I förundersökningen identifierades processen att registrera nya leverantörskonton i Kommers, vilket beskrivs i kapitel 7. Vid registrering inhämtas personuppgifterna genom ett webbformulär som fylls i av skaparen (användaren) av kontot. Skaparen får möjlighet att ge samtycke till att personuppgifterna får användas i marknadsföringssyfte, skaparen får även möjlighet att läsa användaravtalet genom att klicka på en länk innan de godkänner dem. Personuppgifter som behandlas i denna process är de som finns i tabell 8.2

Tabell 8.2 – De behandlade personuppgifterna

Direkta personuppgifter	Indirekta personuppgifter
Förnamn, efternamn och e-mail	Företagets namn och organisationsnummer

Denna data lagras sedan i en databas där den inte är krypterad och alla anställda i organisationen hanterar personuppgifterna från leverantörerna. De använder även missbruksregeln då de behandlar data i ostrukturerad form. De behandlar inte personuppgifter om barn.

11.5.2 Fas II – Riskanalys

En riskanalys gjordes på vad det kan innebära för Infotrust AB att inte vidta åtgärder i processen för att skapa nya konton i leverantörportalen. Följderna till detta blir självklart sanktioner som nämns i kapitel 5.8. Om det blir fulla sanktioner eller om de får milda sanktioner går inte att avgöra just nu, därför diskuteras olika scenarier i senare kapitel. Dessa scenarier tar upp olika sanktionsnivåer till följd av vilka åtgärder som tagits i organisationen. En annan aspekt på detta är att de tappar förtroende från kunderna om de inte lever upp till kraven med GDPR. Genom att inte skydda kundernas personliga integritet kan följden bli att nuvarande och framtida kunder väljer att vända sig till någon annan aktör på marknaden. Att vidta åtgärder bör därför ses som en investering istället för att undvika kostnaden som tillkommer vid dessa åtgärder.

11.5.3 Fas III – Innehåll i implementering

Innehållet i implementationen har beslutats efter hänsyn till avgränsningen, resultatet av förundersökningen och riskanalysen. I processen för att skapa nya leverantörskonton ska åtgärder vidtas för att skydda

personuppgifterna som lagras i databasen, detta ska ske genom att kryptera de direkta personuppgifterna innan de lagras i databasen som medför att den blir oläsbar vid ett eventuellt databasangrepp. Vidare måste förändringar ske angående hur användaren tar del av användaravtal och ger sitt samtycke för behandling av personuppgifterna de lämnar. Lösningarna till dessa beskrivs nedanför i kapitel 8.6. En analys på vad Infotrust AB som organisation behöver vidta för andra åtgärder för att uppnå kraven i GDPR är att utse en ansvarig för implementation, identifiera personuppgiftsbiträde och skriva avtal för hanteringen av de personuppgifter som personuppgiftsbiträdet skall hantera, uppdatera användaravtal och information för inhämtat samtycke, en plan för uppföljning för att kontrollera att GDPR följs efter slutförd implementation och ta fram olika styrdokument.

11.6 Teknisk implementation i en testmiljö

11.6.1 Registrering av leverantörsanvändare

Genom att ändra i kryssrutorna vid registreringen och skapa en funktion som tvingar användaren att läsa användaravtalet som är tydligt och enkelt strukturerat innan de kan registrera kontot. Dessa åtgärder har tagits för att tvinga användaren att ta del av hur deras personuppgifter ska behandlas och till vilket ändamål. Användaren får först ange sina personuppgifter och ge samtycke för de olika behandlingar som står beskrivet vid kryssrutorna innan de går vidare för att registrera kontot. Vid detta steg i processen får användaren upp användaravtalet på skärmen som de måste läsa igenom och längs ner i användaravtalet måste de godkänna detta innan kontot registreras.

11.6.2 Teknisk lösning

Här nedanför i figur 8.2 visas funktionerna som skapades för att tvinga användaren att läsa avtalsvillkoren innan registrering. Funktionen tar fram en popup ruta med användaravtalet och godkännande till samtycke som användaren måste läsa igenom (scrolla igenom avtalen) innan den kan godkänna detta och då bli registrerad som ny användare i portalen. Resultatet av funktionen visas i bilaga D.

```
$(document).ready(function () {
        $(".close").click(function () {
                $('.termsModal').fadeOut('fast');
                $('.overlay').fadeOut('fast');
});

$("#<%=bAcceptTermsAndConditions.ClientID%>").prop("disabled", true)
$('.textBoxHolder').on('scroll', function () {
        if ($(this).scrollTop() +$(this)[0].inner) >= $(this)[0].scrollHeight) {

                $('#<%= bAcceptTermsAndConditions.ClientID %>').prop("disabled", false)
```

Figur 8.2 - Funktion i JavaScript för godkännande av användaravtal

11.6.3 Lagring av personuppgifter

De personuppgifter som leverantören anger vid registrering av nytt konto hanteras i systemet och sparas i databasen. För att skydda den personliga integriteten enligt dataskyddsförordningen har lösningen att kryptera denna data innan den sparas i databasen tagits fram, se Bilaga C. Den data som har valts att kryptera är ett resultat av analysen av personuppgifter som behandlas vid denna funktion i systemet, kryptering av förnamn, efternamn och e-mail hindrar resterande data att relateras till en specifik person och genom detta skydda personens integritet vid intrång. Exempel på en funktion som kan användas vid denna implementation visas nedanför i figur 8.3, figuren visar hur en del av en funktion för RSA-kryptering skriven i språket C#, funktionen visas i sin helhet i Bilaga E[36].

```
        static public byte[] RSAEncrypt(byte[] DataToEncrypt, RSAParame- ters    RSAKeyInfo, bool
DoOAEPPadding)
        {
            try
            {
            byte[] encryptedData;
            //Create a new instance of RSACryptoServiceProvider. using (RSACryptoServiceProvider
            RSA = new RSACryptoServiceProvider())
                {
                //Import the RSA Key information. This only needs
                //toinclude the public key information.
                RSA.ImportParameters(RSAKeyInfo);

                //Encrypt the passed byte array and specify OAEP padding.
                //OAEP padding is only available on Microsoft Windows XP or
                //later.
                encryptedData = RSA.Encrypt(DataToEncrypt, DoOAEPPadding);
                  }
                  return encryptedData;
            }
            //Catch and display a CryptographicException
            //to the console.
            catch (CryptographicException e)
            {
                Console.WriteLine(e.Message);
                return null;
            }
        }
```

Figur 8.3 - Kryptering med RSA skrivet i C#

11.7 Undersökning av ekonomiska påverkan som en implementation skapar

En kostnadskalkyl har gjorts på den tekniska implementationen som denna undersökning behandlar. Kostnaden är beräknad på processen att skapa konto, processen har arbetats igenom tillsammans med lösningsförslaget tills det att den tekniska lösningen är implementerad. En kalkylering har även gjorts på olika nivåer av den sanktionskostnad som kan uppkomma vid utebliven implementation för Infotrust AB utifrån vad förordningen har som riktlinjer. Detta har i denna undersökning delats in i tre olika scenarier vilka diskuteras i kapitel 9. Debiteringskostnaden för utveckling är ett medelvärde som är beräknat på Infotrust AB s egna timdebitering vid konsultuppdrag tillsammans med en ungefärlig timlön för en Infotrust AB anställd som inte är på konsultuppdrag. Denna beräkning har gjorts för att täcka upp en del av intäkterna som uteblir när en konsult jobbar internt och inte är på uppdrag. Tabellerna 8.3 till 8.7 nedan är framtagna för att visa kostnaderna för de olika scenarierna som diskuteras i kapitel 9.

Tabell 8.3 - Kostnad för implementation av lösningsförslag och teknisk implementation (Kronor)

Debiterade timmar	Kr á timme	Kostnad
160 x 2	600	192 000

Tabell 8.4 - Sanktionskostnader för Infotrust AB beroende på sanktionsnivå (Fejkade belopp)

Årsomsättning Infotrust AB år 2016	Sanktionsnivå	Sanktionskostnad
9 123 000	4%	365 000

	3%	274 000
	2%	182 000
	1%	91 000

Tabell 8.5 - Scenario 1 - Enbart implementering av krypteringsfunktioner (Kronor)

Implementationskostnad	114 000
Sanktionskostnad	91 000
Total kostnad	205 000

Tabell 8.6 - Scenario 2 – Endast implementering av förändring för användarvillkorsgodkännandet (Kronor)

Implementationskostnad	78 000
Sanktionskostnad	0
Total kostnad	78 000

Tabell 8.7 - Scenario 3 – Implementering av båda lösningarna (Kronor)

Implementationskostnad	192 000
Sanktionskostnad	0
Total kostnad	192 000

11.8 Kostnadskalkyl företag X

Kostnadskalkyleringen som utfördes hos företag X utfördes i en avgränsad implementation då företag X var i en process av att implementera GDPR i 20 av totalt 48 kritiska system. Kalkyleringen nedanför berör kostnader för att implementera följande förändringar i ett av företag X kritiska system.

- Ta bort känslig personliga data
- Ta bort personliga data i ostrukturerad form
- Hantera accesser (ta bort och lägga till accesser), vilka ska ha tillgång till CRM system
- Kryptering av överföring av data mellan de olika systemen inom företag X
- Skapa en funktion som informerar användarna hur de ska hantera personliga data när de loggar in i systemet

Arbetet med att göra dessa förändringar i detta system har pågått från februari och arbetat med implementationen av GDPR och detta team har bestått av en systemägare, koordinator, teamledare och fem utvecklare.

Tabell 8.8 – Kostnad per timme, roll och spenderad tid hos företag X (Kronor)

Roll	l timme per vecka	Kostnad per timme
Systemägare	4	800
Koordinator	3	800
Teamledare	6	800
Utvecklare	23	800

Tabell 8.9 – Total kostnad och utförda timmar hos företag X (Kronor)

Roll	Totalt utförda timmar	Total kostnad
Systemägare	68	54 400
Koordinator	51	40 800
Teamledare	102	81 600
Utvecklare	391	312 800
Total kostnad		489 600

Företag Y delade inte med sig av siffrorna för implementeringen då de ansåg att det är alldeles för olika bakgrunder mellan företag för att en ekonomisk jämförelse för implementeringen av GDPR skulle ge någonting, speciellt då direktivet inte säger exakt vad man ska göra utan bara vilka frågor man skall lösa.

12 Analys och diskussion

I detta kapitel presenteras egna tolkningar tillsammans med en analys och utvärdering av resultatet som redovisades i kapitel 8. Resultatet kommer att kritiskt diskuteras i jämförelse med alternativa lösningar.

12.1 Definition av personuppgifter

Jag har i resultatet kommit fram till att GDPR:s definition av en personuppgift är väldigt rak och enkel att förstå om du endast skall identifiera direkta eller känsliga personuppgifter. Men enligt de intervjuer och efterforskningar jag gjort i denna undersökning anser jag att svårigheten kommer när indirekta personuppgifter skall identifieras, hur långt skall tolkningen göras och vad anses vara indirekta personuppgifter. Här anser jag att det är oerhört svårt att veta hur långt en identifikation av indirekt data skall dras på grund av att det inte finns tillräckliga riktlinjer för detta. Om jag t.ex. har en bild på ett hus så kan det vara indirekta personuppgifter om den som ser bilden vet vem som bor i huset men när andra människor ser bilden så är det bara ett hus och ingenting annat, är detta då indirekta personuppgifter när enbart en eller ett fåtal som kanske aldrig kommer se bilden kan identifiera en person? Det här är frågor som organisationer kommer behöva ställa sig då riktlinjerna i förordningen inte är tillräckliga.

12.2 Intervjuer

De företagen som intervjuades var två helt skilda företag, både i storlek och vad de har som affärsidé. Detta medförde att de bemöter implementationen av GDPR på två olika sätt. Som beskrivet i metoden så var intervjuerna semistrukturerade och detta gav möjligheten att validera den checklista som jag tagit fram. Båda företagen har delat upp implementationen i faser som liknar de faser som finns i vår checklista. Båda anger t.ex. att de har valt att utbilda sin personal, analysera de olika processer de har och identifiera personuppgifter i dessa för att senare gå vidare till en riskanalys och sedan skapa en uppfattning om vad de behöver göra för förändringar för att möta GDPR:s direktiv. Detta anser jag ge en validitet till den checklista som arbetats fram i denna undersökning då bl.a. faserna och identifikationerna är liknande. Det skulle kunna argumenteras för att valideringen bör vara starkare, då det inte finns någon exakt specifikation att följa eller någon praxis från ärenden hos Datainspektionen så måste detta anses vara tillräckligt vid tidpunkten då denna undersökning utfördes.

12.3 Generell plan för implementering

I detta delkapitel så diskuteras de faser och checklistan i den generella planen som tagits fram i denna undersökning. Hur det är tänkt att den skall användas och hur den är uppbyggd. Varför den är framtagen som en generell plan och inte specifika uppgifter. Planen diskuteras även kritiskt för att försöka få en bild av var den skulle kunna bli starkare.

12.3.1 Fas I

Det kan diskuteras om det finns tillräckligt många punkter i förundersökningen för att göra en total analys över organisationen. Jag anser att identifikation av funktioner och processer är en central del för att kunna hantera en implementation av GDPR, jag har dock valt att inte gå in på djupet i vad som kan vara en process då en organisation aldrig är den andra lik. Jag vill få organisationen att tänka till själva för att på så sätt lyckas identifiera alla processer som behandlar personuppgifter. Förundersökningen i lösningsförslaget är skapad för att få organisationen att förstå innebörden av GDPR, tanken är att genom detta så skall organisationen ta in kunskap som gör att identifieringen av problemområden blir lättare. De andra två punkterna är enbart till som stöd för att ge organisationen en uppfattning om vad de skall identifiera i de olika processerna för att på så sätt veta om processen måste hanteras. Detta kompletteras med en checklista med fler frågor som en organisation kan ställa sig i sökandet efter de berörda processerna. Precis som att en organisation aldrig är den andra lik så kommer en slutgiltig lista över processer aldrig se likadan ut, därav tar checklistan upp frågor som denna undersökning anser vara generella frågor som förmodligen finns i alla organisationer. Målet är att organisationen med detta skall kunna identifiera alla sina processer och inte enbart de självklara.

12.3.2 Fas II

Riskfasen är svår att ge vägledning inom då denna är baserad på förundersökningen och hur organisationen ser ut. Men jag anser att när man gjort förundersökningen skapar det en kunskap inom GDPR och vilka risker som organisationen kan utsättas för. Detta går hand i hand med det risktänk som GDPR vill ta fram hos

organisationer för att kunna hantera den personliga integriteten på ett bra sätt. Det är på grund av detta det inte togs fram tydligare riktlinjer på vad för risker organisationen ska analysera i Fas II och att det är helt beroende på vad för verksamhet organisationen driver. Styrkan i denna undersökning är att det finns grundfrågor i checklistan som kan ge vägledning om vilka risker som kan finnas och på så sätt starta risktänket hos organisationen.

12.3.3 Fas III

Denna fas består av innehållet i implementationen och är ett resultat av förundersökningen och riskanalysen, här har jag tagit fram delar som är ett krav enligt GDPR som varje organisation måste hantera vid införandet av GDPR, dessa delar är specificerade i checklistan. Utöver detta tillkommer de förändringarna som identifierades i resultat av förundersökningen och riskanalysen. En fråga som alla organisationer kommer att bli tvingade att hantera är hur de ska hantera ostrukturerade data då det inte finns några riktlinjer på hur detta ska behandlas. Tidigare kunde denna punkt undvikas genom missbruksregeln som nu försvinner. Då jag blivit tvingade att göra avgränsningar, har jag i denna undersökning inte hittat en lösning på att hantera ostrukturerade data. Diskussioner angående detta har först under undersökningens gång och en tanke jag har för att hantera ostrukturerade data är att tänka privacy by design vid utvecklande av nya eller befintliga processer. Genom detta lyfts frågan fram tidigt i processen för att hantera detta på bästa sätt.

12.3.4 Teknisk lösning

Åtgärder för att säkerställa att användaren tar del av användarvillkoren

Rullningsfunktionen säkerställer att användaren tagit del av användarvillkoren och givit sitt samtycke till organisationens behandling av personuppgifter. Att användaren blir tvingad att scrolla igenom användaravtalet och klicka godkänn medför att användaren får alla möjligheter att förstå hur organisationen behandlar personuppgifterna.
Jag ansåg att rullningsfunktionen är en central del i lösningen för att tvinga användaren att ta del av användarvillkoren. Något jag anser kan skapa förvirring är om användaren inte förstår att knappen för att godkänna avtalet aktiveras förrän efter att man scrollat igenom texten, argumentet för att ändå använda denna metod grundar sig i att i dagens samhälle har majoriteten av användarna god datorvana och att det är underförstått att knappen inte aktiveras förrän man har scrollat igenom texten. Det finns även en risk att användaren inte läser igenom användaravtalen utan enbart scrollar ner och godkänner avtalet. Men jag anser att denna lösning uppfyller de direktiv enligt kapitel III, artikel 12 i förordningen. *”Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn”*.

En alternativ lösning är att utgå från den ursprungliga metoden med en kryssruta och bredvid denna kryssruta en länk till användarvillkoren, här kan då en funktion införas som inte aktiverar kryssrutan förrän att användaren har klickat på länken för användarvillkoren. Detta skulle då behöva förtydligas med en förklarande text vid kryssrutan. Med denna lösning anser jag att det finns en stor risk att användaren endast klickar på länken och inte tittar på användaravtalen och därför bestämde jag oss för att använda den förstnämnda lösningen.

12.3.5 Kryptering

Den lösningen jag har tagit fram som förslag är att skydda de direkta personuppgifterna med kryptering och genom krypteringen stoppa identifikationen av en person genom indirekta personuppgifter. Då de indirekta personuppgifterna som identifierades i processen att skapa nytt konto består av företagsuppgifter, anser jag att de direkta personuppgifterna skall krypteras för att då hindra en identifikation av en specifik person genom företagsuppgifter som finns lagrade. Jag valde att ge förslaget att kryptera informationen i webbapplikationen för att inte bli hindrade av en databashanterares egen krypteringsalgoritm. (Detta sett utanför ramen av SSL/TLS). Detta ger en styrka och valfrihet i att olika algoritmer kan väljas beroende på vilken säkerhetsnivå man vill ha och dessutom finns valmöjligheten att byta krypteringsalgoritm i framtiden för att öka säkerheten om det behövs. Genom denna lösning anser jag att den personliga integriteten är skyddad vid ett databasangrepp då specifika personer inte går att identifieras om de kommer över den data som finns i databasen. Då krypteringen sker i applikationslagret måste även dekrypteringen ske i applikationslagret vid alla

de funktioner som behandlar denna data. Jag anser att dessa funktioner endast behöver anropa dekrypteringsfunktionen som skapas i samband med krypteringen. Det som kan vara problematiskt är att identifiera vilka funktioner som behöver använda sig av kryptering och dekryptering. Här anser jag att dessa funktioner redan bör vara identifierade under förundersökningen och denna lista med processer kan då återanvändas för att identifiera vilka som dessutom kommer kräva kryptering eller dekryptering. En alternativ lösning är att dela upp direkta och indirekta personuppgifter i två olika databaser. Genom detta kan inte de indirekta personuppgifterna kopplas till en person om det endast sker ett databasintrång i en av databaserna. Nackdelen är att om det sker i den databasen med de direkta personuppgifterna så kan angriparen identifiera personerna direkt. För att undvika detta kan ytterligare en säkerhetsåtgärd vidtas, att kryptera de direkta personuppgifterna i databasen som anges till första lösningen.

12.4 Ekonomisk beräkning

Den tekniska implementationen i kapitel 8.6 är från ett ekonomiskt perspektiv enbart en kostnad, det finns inga möjliga intäkter kopplade till den då funktionen är ett grundläggande krav från GDPR. Det ska tas i beaktande att denna implementering inte är en fullständig implementering utan enbart en liten del, detta medför att kostnaden för en total implementation kommer vara mycket högre. Men det kan enligt oss ses som en kostnadsbesparing gentemot att riskera stora och dyra sanktioner från Datainspektionen vid utebliven implementering.

Vid en eventuell personuppgiftsincident kan kostnaderna för organisationerna bli väldigt höga då de riskerar en väldigt stor sanktionsavgift utöver detta så kan det även vid fall där en registrerad åsamkats skada bli tal om skadestånd. Det skulle även kunna tillkomma jurist och rättegångskostnader, det är dock någonting jag valt att inte ta med i beräkningarna då de efterforskningar jag har utfört hos jurist och advokatbyråer gett så blandade och osäkra resultat.

Jag gjorde en beräkning på de tekniska lösningarna och implementation i Kommers och jämförde den med kostnaden vid en eventuell personuppgiftsincident. Vid kostnadsberäkningen för en incident så räknade jag på olika sanktionsnivåer, juristkostnader och skadestånd till den utsatte. Om en incident sker som Datainspektionen anser vara av den grad att en sanktionsavgift behövs då kommer förutom den kostnaden även kostnaden för implementering också tillkomma för att lösa problemet som Datainspektionen säger finns. Jag anser efter en jämförelse att det är mest kostnadseffektivt att implementera en lösning nu före den 25 maj 2018 då organisationen annars med all säkerhet kommer riskera att en incident sker och att Datainspektionen då kommer ge en reprimand och tvinga en implementering att utföras och dessutom en riskerad sanktionsavgift och ett skadestånd till de utsatta.

12.4.1 Scenarios

Jag har valt ut några scenarion för att visa upp varför man som organisation bör göra investeringar för att implementera GDPR. Som kan ses i tabellen i kapitel 8.7 finns en sanktionsavgift på 4% av årsomsättningen, detta skulle i Infotrust AB s fall ersättas med 20 000 000 € i sanktionsavgift enligt förordningen vilket är detsamma som konkurs, av anledning att en jämförelse med detta i alla tänkbara fall tyder på att man skall göra alla implementationer man kan tänka sig då bortser jag helt från att använda detta scenario.

12.4.2 Scenario 1 - Endast implementering av krypteringsfunktioner

Det första scenariot som jag tittat på är att enbart implementera krypteringsfunktionen där förnamn, efternamn och e-mailadress krypteras. Denna funktion har som tabellen i resultatet visar en relativt hög kostnad då val av krypteringsalgoritm och var i systemen den faktiska krypteringen skall ske inte är helt enkel. Om enbart denna implementation utförs så anser jag att företaget gjort en förundersökning på vad som behöver göras för att möta GDPR:s krav och dessutom infört en form av skydd för personuppgifterna som lagras. Detta borde visa vid en personuppgiftsincident att företaget försökt minska risken för den registrerade och detta borde enligt förordningen ge enbart en mindre sanktion. Då organisationen inte har tagit till åtgärder för att samla in samtycke från den registrerade ser jag på det som att detta är ett tillräckligt snedsteg för att riskera en lägre summa i sanktion. Kostnaden för att implementera krypteringsfunktioner och eventuell uppskattad sanktionskostnad blir högre jämfört med att implementera både kryptering och förändringen av användarvillkorsgodkännandet. Därmed anser jag att det är mer lönsamt att implementera båda lösningarna.

12.4.3 Scenario 2 - Endast implementering av förändring för användarvillkorsgodkännandet

Vid en eventuell implementering av förändringen i hur samtycke inhämtas som visas i kapitel 8, ser jag att kostnaden för implementationen är lägre än i scenario 1. Detta beror på att funktionen inte kräver lika mycket arbete som en krypteringsalgoritm kräver för att implementeras, dock anser jag efter tolkning av förordningen att denna funktion är oerhört central, att den registrerade får möjligheten att läsa in sig på hur personuppgifterna kommer att lagras är en av de viktigaste delar som GDPR har tagits fram för att hantera. Eftersom samtycket är väldigt centralt anser jag att detta tillsammans med att checklistan följs i resterande delar i denna process bör minimera risken för sanktioner från datainspektionen i Infotrust AB s fall.

12.4.4 Scenario 3 – Implementering av båda lösningarna

Att implementera båda lösningarna kan från början tänkas vara onödigt då scenario 2 säger att organisationen bör slippa kostnaden för en sanktion och det finns en besparing i att inte implementera krypteringen. Dock skall man se till att om scenario 2 faller in och en reprimand från datainspektionen kommer då kan denna tänkas innehålla att vidta åtgärder för att skydda de personuppgifterna och den åtgärden som jag har tagit upp här är att kryptera. Då ser jag i efterhand att båda kostnaderna kommer infinna sig ändå och jag anser då att om möjligheten att undvika sanktioner helt finns så bör dessa vidtas från början.

12.4.5 Kostnadsjämförelse med kostnadskalkyl för företag X och Y

Tabell 9 visar på en prisskillnad på cirka 300 000 kr för en implementering hos företag X jämfört med Infotrust AB. Det kan tyckas vara en stor skillnad i summor men implementeringen som har utförts på företag X är större än implementeringarna utförda i Infotrust AB s system, för att införa samma saker hos Infotrust AB så skulle kostnaden gå upp och närma sig varandra avsevärt. Då Företag X har 20 stycken liknande projekt igång och dessa beräknas kosta ungefär lika mycket så styrker detta att Infotrust AB rent marknadsmässigt borde utföra de implementeringar som tagits fram i denna undersökning då kostnaden är i samma intervall som hos företag X som har gjort en utförlig förundersökning och marknadsanalys.

Företag Y diskuterade enbart strukturkapital och ansåg att summan för en implementering av GDPR inte går att beräkna rakt av då det hos dem tillkommer kostnader för implementering av nya system som utförs samtidigt för att kostnaden för den implementeringen minskar i och med att GDPR-implementeringen redan utförs. Att det redan investerade strukturkapitalet i personuppgiftslagen skiljer sig väldigt mycket mellan aktörer på marknaden är även detta ett incitament för att en ekonomisk jämförelse blir svår att skapa på ett korrekt sätt.

12.5 Hållbarhet

Med införandet av GDPR tvingas företagen att vidta striktare åtgärder för att skydda den personliga integriteten. Eftersom att GDPR är ett EU direktiv stärks medborgarens rättigheter i ett bredare och mer hållbart vis gentemot tidigare lösning som baserades på den lagen som i Sverige heter PUL, medlemsländerna tolkade PUL olika och detta medförde att personuppgifterna hanterades på olika vis beroende på vilket medlemsland som hanterade uppgifterna. Då utveckling i dagens informationssamhälle sker i en hög takt och på sättet digitaliseringen har tagit fart i de flesta företagen medför detta risker för den registrerade då ett dataintrång gör större skada i dagens samhälle jämfört med när PUL infördes. Hållbarhetsutmaningen blir större och detta måste hanteras globalt, på ett gemensamt sätt. Införandet av GDPR är ett stort steg i rätt riktning då även icke EU-medlemmar som hanterar uppgifter från något av länderna där GDPR har införts måste hantera dessa uppgifter på samma sätt som EU-medlemmar. Detta kan i sin tur vara en utgångspunkt för att övriga länder stärker kraven för hur hantering av data skall ske inom sina egna gränser. GDPR ställer även kravet att tydligt kommunicera hur personuppgifterna kommer hanteras för de berörda, detta skapar då medvetenhet hos den enskilda personen om vad den ger medgivande till och möjligheten att kontrollera hur deras personuppgifter skall behandlas. Att GDPR införs är inte enbart positivt för den enskilda personen, företagen blir mer transparenta på hur personuppgifterna skall behandlas vilket medför till att kunden blir tryggare som i sin tur leder till att kunderna uppskattar företagen mer och detta stärker företagets varumärke då de kan visa att de bryr sig om sina kunder.

13 Slutsats och rekommendationer

Målsättningen att ta fram en generell plan och en generell specifikation har uppnåtts i denna undersökning genom att en lösning är framtagen som ett stöd för en organisation som är i början av processen att implementera GDPR. Den ska hjälpa organisationerna att komma igång med projektet och ställa de centrala frågorna kring GDPR. Efter resultatet från intervjuerna, information från seminarier och analysen av Infotrust AB har undersökningen kommit fram till att en organisation bör utvärdera om checklistan har tillräckligt med frågor för att täcka hela organisationens behov och beroende på utfallet tillägga eller ta bort frågor i checklistan.

Lösningsförslaget som är framtaget i denna undersökning har applicerats på en avgränsad del hos Infotrust AB där det gett positiva resultat. Genom att applicera det framtagna lösningsförslaget hos Infotrust AB och genom de intervjuer som utfördes tidigare i undersökningen så anser jag att resultatet är positivt och att lösningsförslaget även kan användas i andra processer och i andra organisationer. Jag tog fram en checklista under undersökningen och trovärdigheten i denna har arbetats fram med grunden i datainspektionens riktlinjer. Dessa har kompletterats med resultatet från egna undersökningar och de intervjuer som utfördes under undersökningen. Målsättningen att studera vad personliga data är anses vara uppnådd och resultatet har gett en större möjlighet att använda lösningsförslaget på ett tydligare sätt vilket förkortade tiden det tog för identifieringen av personuppgifter i processen. Den ekonomiska målsättningen att utvärdera kostnaden för en implementering ställd mot att inte utföra denna implementering kan anses vara uppnådd. Dock skall det tas i beaktande att undersökningen visar att förordningen är framtagen för att tvinga en organisation att göra de nödvändiga implementeringarna då kostnaderna enligt denna undersökning annars alltid kommer vara högre om en implementering inte utförs vilket innebär att en rekommendation att göra implementationen kommer vara ett krav från den ekonomiska undersökningen.

Företag Y anser att det är oerhört svårt att göra ekonomiska jämförelser inom ämnet då det är stora skillnader i vilket läge som de jämförda företagen befinner sig i. Det kan skilja i hur hanteringen av personuppgifter har varit och vilken storlek samt vilken marknad företagen verkar på. Efter de intervjuer som utfördes hos företag X och Y anser jag att beräkningen som jag utfört hos Infotrust AB anses vara rimlig då företag X verkar inom IT-marknaden precis som Infotrust AB och de har inte en enorm hantering av personuppgifter, även detta i likhet med Infotrust AB. De mindre projekten som företag X nu använder sig av för att säkra sig mot GDPR är i samma storleksordning som en implementering hos Infotrust AB medför att jag anser att dessa kan jämföras med varandra då kostnaderna korrelerar med varandra.

Den här undersökningen ger ingen lösning till hur ostrukturerade data skall hanteras, då detta är en fråga som är oerhört viktig inom GDPR måste en vidare undersökning i detta ämne utföras. Då denna undersökning är utförd före den 25 maj 2018 så bör det tas i beaktande att det kan komma skarpa uppdateringar från datainspektionen som inte studerats nu.

14 Referenser

2http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204

3 https://europa.eu/european-union/eu-law/legal-acts_sv

4 https://unstats.un.org/sdgs/indicators/database/?indicator=17.8.1

5https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivlag- 1990782_sfs-1990-782

6https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk- forfattningssamling/bokforingslag-19991078_sfs-1999-1078

7 http://www.Infotrust AB .se/sv/hem/

8 https://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-en-personuppgift/

9https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/kansliga- personuppgifter-uppgifter-om-brott-och-personnummer/detta-ar-kansliga-personuppgifter/

10 https://developer.mozilla.org/en-US/docs/Learn/JavaScript/First_steps/What_is_JavaScript

11https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk- forfattningssamling/tryckfrihetsforordning-1949105_sfs-1949-105

12https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/yttrandefrihetsgrundlag-19911469_sfs-1991-1469

13 https://it-ord.idg.se/ord/ansvarig-utgivare/

14 https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

15 https://sv.wikipedia.org/w/index.php?title=RSA&oldid=40916360

16https://msdn.microsoft.com/en-us/library/system.security.cryptography.rsacryptoserviceprovider(v=vs.110).aspx?cs-save- lang=1&cs-lang=csharp#code-snippet-2

17https://docs.microsoft.com/en-us/dotnet/csharp/getting-started/introduction-to-the-csharp- language-and-the-net-framework

18 http://csharpskolan.se/article/introduktion-till-net

19 https://en.wikipedia.org/w/index.php?title=Electronic_discovery&oldid=820657934

20 https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#1

21https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk- forfattningssamling/bokforingslag-19991078_sfs-1999-1078

22https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivlag- 1990782_sfs-1990-782

23https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#9

24https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#K3

25https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de- registrerades-rattigheter/ratt-till-radering/

26https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de- registrerades-rattigheter/ratt-till-begransning-av-behandling/

27https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de- registrerades-rattigheter/ratt-till-information/

28https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de- registrerades-rattigheter/dataportabilitet/

29https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#4

30https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#28

31 https://www.datainspektionen.se/Documents/Riktlinjer%20om%20dataskyddsombud.pdf

32https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#K5

33https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#K9

34 https://www.datainspektionen.se/utbildning/

14.1 Källförteckning

1. C. Tankard, ”What the GDPR means for businesses”, *Netw. Secur.*, vol. 2016, nr 6, s. 5–8, juni 2016.
2. S. Mansfield-Devine, ”Meeting the needs of GDPR with encryption”, *Comput. Fraud Secur.*, vol. 2017, nr 9, s. 16–20, sep. 2017.
3. H. Månsson och J. Erichsen, ”Tillmötesgåendet av GDPR - Utmaningar ur ett tekniskt och processorienterat perspektiv”, Kandidatexamenuppsats, Lunds Universitet- Institution för informatik, 2017.
4. L. Ryz och L. Grest, ”A new era in data protection”, *Comput. Fraud Secur.*, vol. 2016, nr 3, s. 18–20, mar. 2016.
5. S. Adolfsson och P. Lundholm, ”Detaljhandelns förberedelser inför GDPR : En fallundersökning om vilka förändringar företagen behöver utföra samt deras arbete kring GDPR”, Kandidatexamensuppsats, Uppsala Universitet, http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1112096&dswid=5860, [Åtkomstdatum: 20-feb- 2018].
6. K. Pormeister, ”The GDPR and Big Data: Leading the Way for Big Genetic Data?”, i *Privacy Technologies and Policy*, 2017, s. 3–18.
7. J. Pettersson och M. Brädefors, ”Det är inte lagarna som passerar, det är lagarna jag minns : hur företag förbereder sig inför de förändringar som införandet av GDPR innebär”, Kandidatexamenuppsats, Uppsala Universitet, http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-340743, [Åtkomstdatum: 02-Mars-2018].
8. Smouter Kim, ”The Year of the GDPR”, *Res. World*, vol. 2018, nr 68, s. 48– 49, feb. 2018.
9. D. Stark, B. Reg, och Q. Ashlin, ”ESOMAR Data Protection Checklist”, ESOMAR - World Research codes and guidelines.
10. H. Gjermundrød, I. Dionysiou, och K. Costa, ”privacyTracker: A Privacy-by- Design GDPR-Compliant Framework with Verifiable Data Traceability Controls”, i *Current Trends in Web Engineering*, 2016, s. 3–15.
11. Lagtext, Datainspektionen, ”Dataskyddsförordningen - texten i sin helhet - Datainspektionen”. [Online]. Tillgänglig vid: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningst exten/. [Åtkomstdatum: 09-feb-2018].
12. Alan Bryman, Social Research Methods, Fourth edition., vol. 2012. Oxford University Press
13. M. Denscombe, The Good Research Guide, For small-scale social research projects, Fifth edition., vol. 2015. McGraw-Hill Open University Press.

15 Bilagor

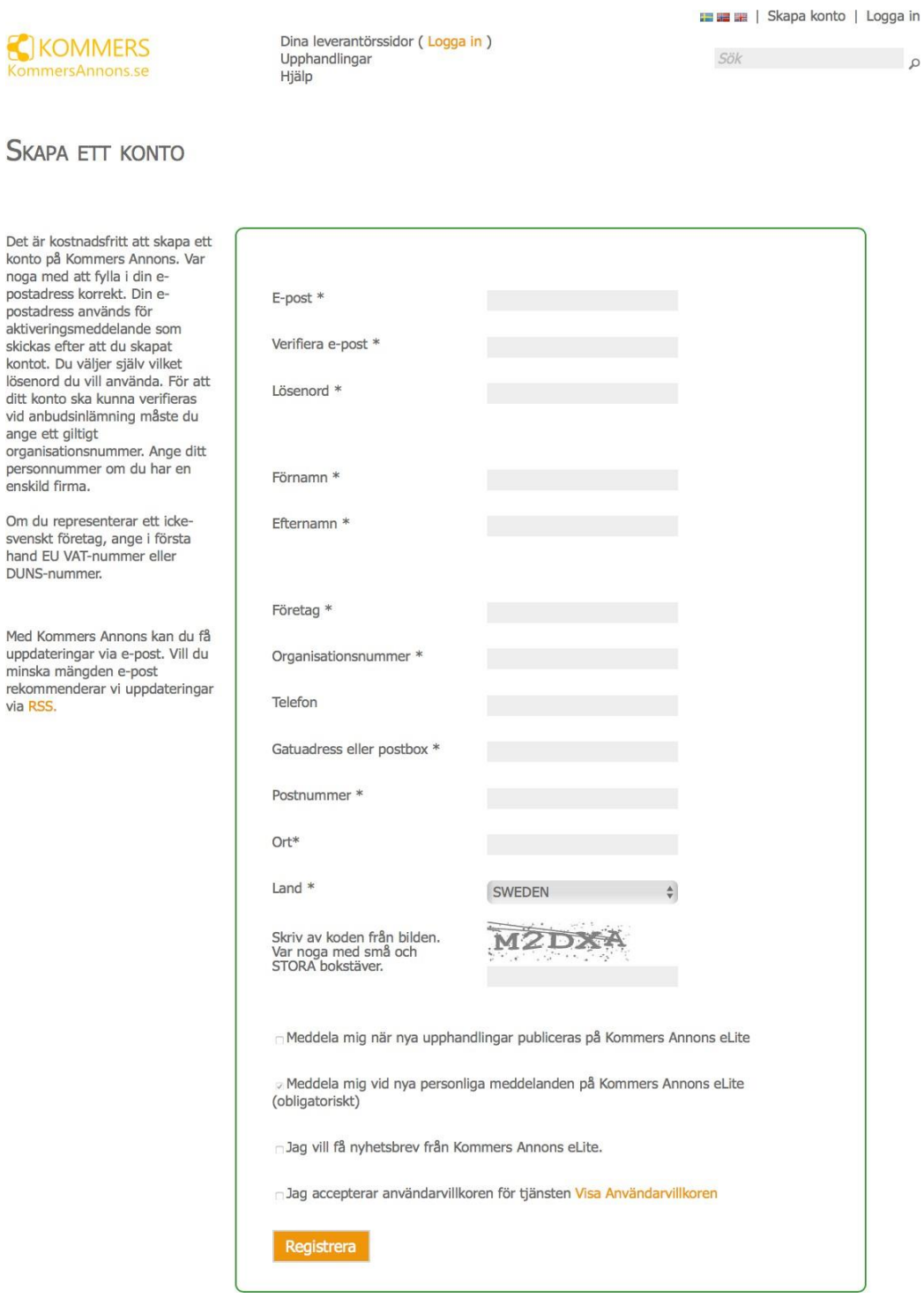
15.1 Bilaga A - Checklista för implementation av GDPR

Den vänstra kolumnen kan innehålla tre olika bokstäver S, D, I som refererar till källan som har tagit fram frågan i checklistan. S - Denna undersökning, D - Datainspektionen och I - Intervjuer från denna undersökning. Vissa punkter är framtagna i kombination av resultat av denna undersökning och information från datainspektionen.

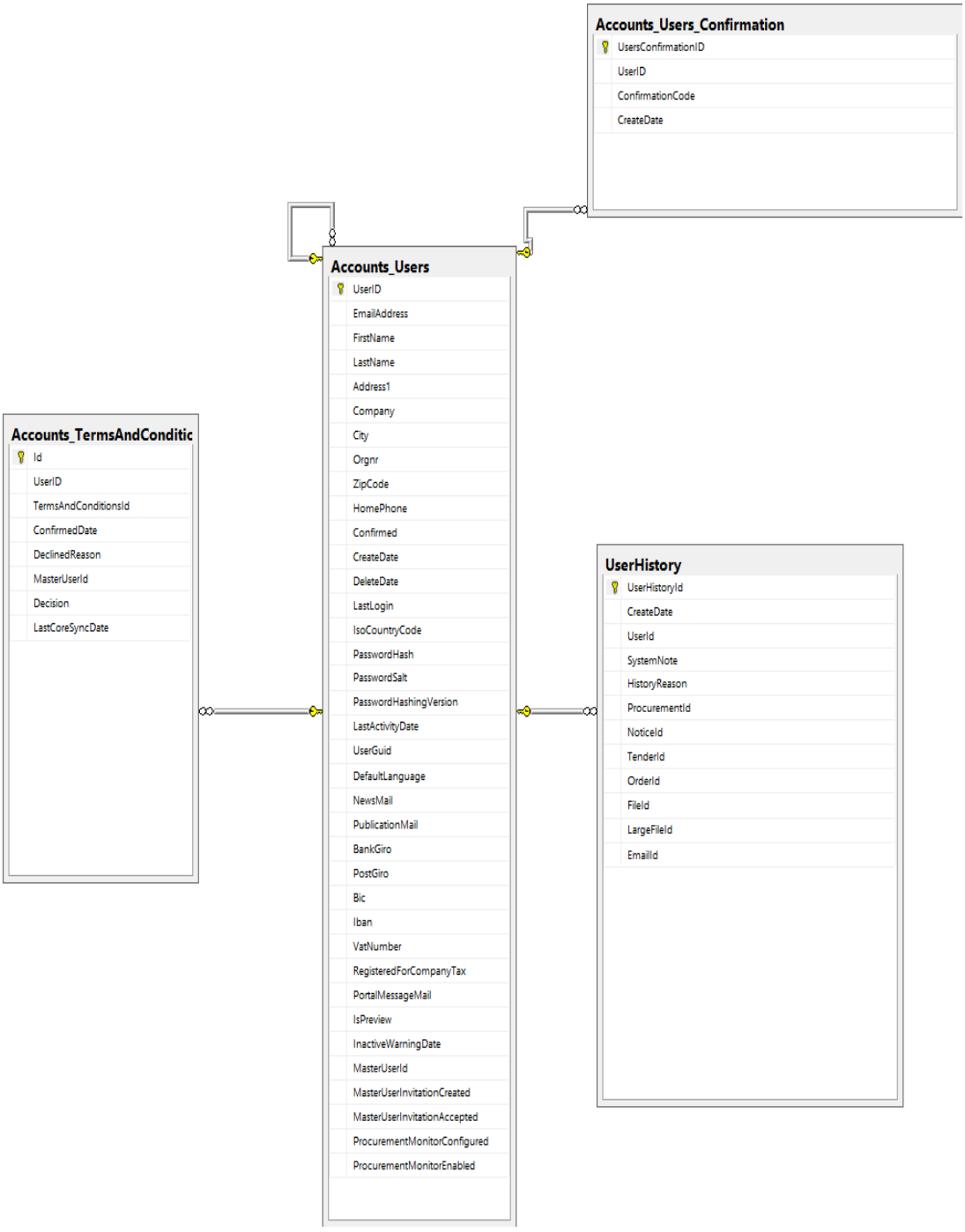
	Fas I - Förundersökning	**Resultat av analys**
S	Läsa in om vad GDPR är och förstå hur ni måste förhålla er till kraven i dataskyddsförordningen.	
S	Vilka funktioner och var hanterar ni personliga data (processer)	
S	Interna processer som behandlar personuppgifter	
D	Tredje parts behandling av personuppgifter	
D S	Identifiera och kartlägg vilka personuppgifter ni hanterar.	
D S	Skapa ett register över vilken typ av personuppgifter som behandlas och till vilket ändamål	
S	Dela upp i indirekt och direkt identifierande data	
D	Hur sker insamlingen av personuppgifter?	
S I	Hur lagrar ni personuppgifter som ni inhämtat?	
S	Vilka personer hanterar personuppgifter?	
D	Använder ni missbruksregeln idag?	
D	Hur och vad lämnar ni för information om hanteringen av personuppgifter till kunderna idag?	
D	Behandlar ni personuppgifter om barn under 16 år (13 år enligt förslag för Sverige)?	
	Fas II - Risker	**Resultat av analys**
S I	Analysera riskerna för företaget med att inte vara ”GDPR-ready”	
D S	Kan företaget identifiera integritetsintrång?	
S I	Hur påverkas företaget av ett integritetsintrång?	
S I	Kan ni hantera personuppgiftsförfrågningar som tillkommer i och med den nya förordningen? (Registerutdrag, Ändring, förflyttning, radering)	
S I	En konsekvensbedömning om vad för följder som tillkommer om företaget inte har tillräckliga åtgärder för att hantera personuppgifter	
	Fas III - Innehåll i implementering	**Resultat av analys**
S	Utse en ansvarig för genomförandet av implementationen	
D	Utse dataskyddsombud	
D	Utse personuppgiftsbiträde	
D S	Vilka åtgärder behöver vidtas i systemet och de processer som finns?	

S	Uppdatera användaravtal och information för att inhämta samtycke	
D **S**	Framställ ett dokument med en plan för att kontrollera att GDPR följs efter slutförd implementation	
S	Ta fram eller uppdatera rättsliga dokument (t.ex. användaravtal och leverantörsavtal)	
D **S**	Skapa styrdokument för hur personalen skall hantera persondata.	
D **S**	Skapa styrdokument för hur personalen skall agera vid en personuppgiftsincident eller misstanke om incident har identifierats.	
D **S**	Skapa styrdokument för hur en personuppgiftsincident skall bedömas.	
D **S**	Skapa styrdokument för hantering av utdrag av personliga data som företaget har om kunden vid kundens begäran.	
D **S**	Skapa styrdokument för hantering av radering av personuppgifter på kundens begäran.	
D **S**	Skapa styrdokument för hantering av dataportabilitet.	
D	Skapa utbildningspaket för personal beroende på vad för arbetsuppgifter de har.	
S		
D **S**	Ta fram raderingsrutiner - Företagets egna rutiner för hur radering skall ske fortlöpande enligt gällande lagar och avtal.	
D **S**	Skapa transparent användargränssnitt mot kund om möjligt och ekonomiskt försvarbart	

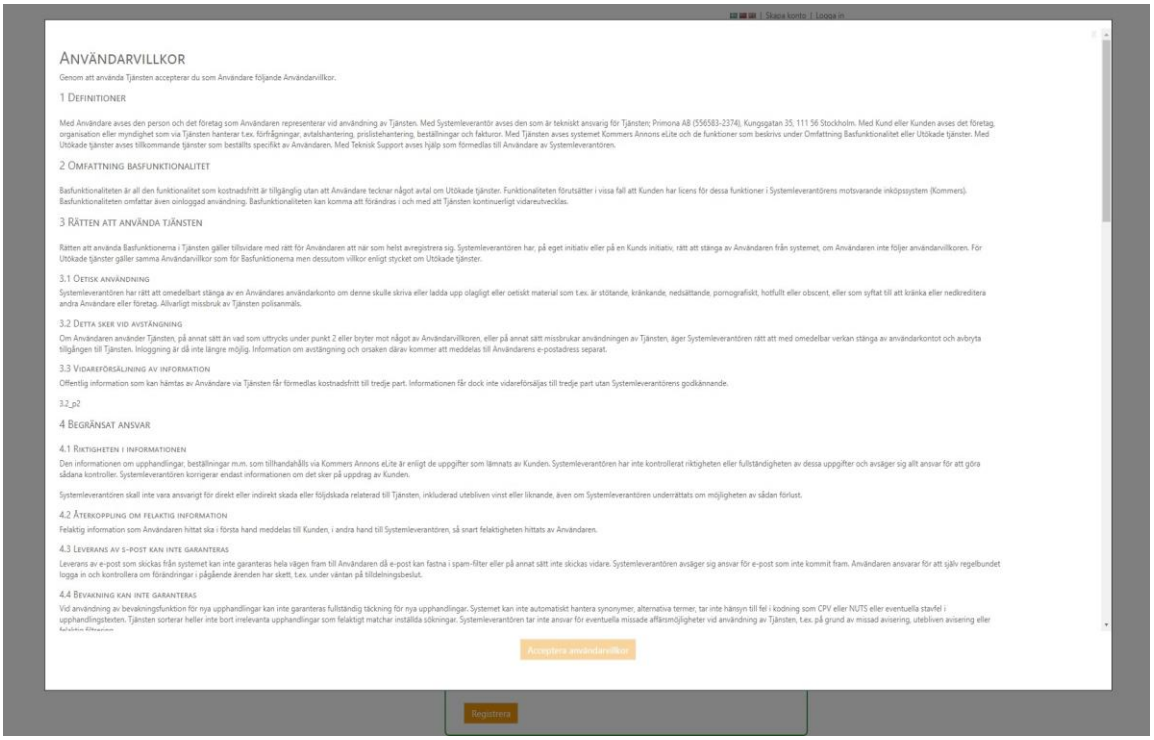
15.2 Bilaga B – Skapa leverantörskonto (före implementation)



15.3 Bilaga C – Databasstruktur för att registrera nytt leverantörskonto



15.4 Bilaga D – Resultat av implementation för godkännande avtalsvillkor



15.5 Bilaga E – RSA kryptering

```
using System;
using System.Security.Cryptography; using System.Text;
class RSACSPSample
{
static void Main()
{
try
{
//Create a UnicodeEncoder to convert betweenbyte array and string.
UnicodeEncoding ByteConverter = new UnicodeEncoding();
//Create byte arrays to hold original, encrypted, and decrypted data.
byte[] dataToEncrypt = ByteConverter.GetBytes("Data to Encrypt"); byte[] encryptedData;
byte[] decryptedData;
//Create a new instance of RSACryptoServiceProvider to generate
//public and private key data.
Static public byte[] RSAEncrypt(byte[] DataToEncrypt, RSAParameters
RSAKeyInfo, bool DoOAEPPadding)
{
try
{
```

```
byte[] encryptedData;
//Create a new instance of RSACryptoServiceProvider.
using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
{
//Import the RSA Key information. This only needs
//toinclude the public key information. RSA.ImportParameters(RSAKeyInfo);
//Encrypt the passed byte array and specify OAEP padding.
//OAEP padding is only available on Microsoft Windows XP or
//later.

encryptedData = RSA.Encrypt(DataToEncrypt, DoOAEPPadding);
}
return encryptedData;
}
//Catch and display a CryptographicException

//to the console.
catch (CryptographicException e)
{
try
{
//Create a new RSACryptoServiceProvider object.
using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
}
//Export the key information to an RSAParameters object.
//Pass false to export the public key information or pass
//true to export public and private key information.
```