



HÖGSKOLAN  
DALARNA

## Examensarbete

Kandidatexamen

### **Organisationers utmaningar och åtgärder vid framtagandet av samtyckestexter samt dess behandling av personuppgifter i enlighet med dataskyddsförordningen (GDPR)**

---

#### **Organizations challenges and actions in the development of consent documents and their processing of personal data in accordance with the General Data Protection Regulation (GDPR)**

Författare: Tesfaom Alem & William Lind

Handledare: Johan Håkansson

Examinator: Anders Avdic

Ämne/huvudområde: Informatik

Kurskod: IK2017

Poäng: 15 högskolepoäng

Ventilerings-/examinationsdatum:

Vid Högskolan Dalarna har du möjlighet att publicera ditt examensarbete i fulltext i DiVA. Publiceringen sker Open Access, vilket innebär att arbetet blir fritt tillgängligt att läsa och ladda ned på nätet. Du ökar därmed spridningen och synligheten av ditt examensarbete.

Open Access är på väg att bli norm för att sprida vetenskaplig information på nätet. Högskolan Dalarna rekommenderar såväl forskare som studenter att publicera sina arbeten Open Access.

Jag/vi medger publicering i fulltext (fritt tillgänglig på nätet, Open Access):

Ja

Nej

## **Sammanfattning**

Utvecklingen av digital teknik tillsammans med nya affärsmodeller har nått nya nivåer under de senaste åren vilket har resulterat i att behandlingen av personuppgifter både ökat och förändrats. Problematiken med detta innefattar att den personliga integriteten i större utsträckning kränks. I syfte att harmonisera behandlingen av personuppgifter och att stärka skyddet av den personliga integriteten har EU infört en ny dataskyddsförordning. Förordningen träder i kraft den 25 maj 2018 och ska tillämpas i nationell lagstiftning vilket gör att den svenska personuppgiftslagen ersätts.

Syftet med studien var att identifiera vilka åtgärder ett antal organisationer vidtagit för att följa dataskyddsförordningens regler samt vilka utmaningar som kan uppstå i omställningen. Studien är avgränsad till samtyckestexter och behandling av personuppgifter. Studien är kvalitativ och vi har med hjälp av intervjuer tagit del av ett antal organisationers syn på utmaningar och åtgärder gällande formuleringar av samtyckestexter och dess personuppgiftsbehandling.

Slutsatsen i denna studie visar att samtliga organisationerna har problem att formulera samtyckestexter på ett informativt sätt vilket dataskyddsförordningen kräver. Organisationerna ser även utmaningar i behandlingen av personuppgifter. Dessa utmaningar består av komplexa IT-system innehållande mängder av personuppgifter som idag inte kan hanteras i enlighet med dataskyddsförordningen då relevant systemstöd saknas.

## **Nyckelord**

GDPR, Dataskyddsförordningen, Personuppgiftslagen, Samtycke, Personuppgiftsbehandling

## **Abstract**

The rapid development of digital technology together with new business models has reached new levels in recent years, which has resulted in the processing of personal data both increasing and changing. The problem with this development involves the violation of personal integrity to a greater extent. In order to harmonize the processing of personal data and to strengthen the protection of personal privacy, the EU has introduced a new data protection regulation. The regulation will enter into force on May 25, 2018 and will apply in national legislation, which will replace the Swedish Personal Data Act.

The purpose of the study was to identify what measures a number of organizations have taken to comply with the rules of data protection regulations and the challenges that may arise in the conversion. The study is limited to consent texts and processing of personal data. The study is qualitative and we have, through interviews, taken note of a number of organizations' views on challenges and measures regarding formulas of consent texts and their personal data processing.

The conclusion in this study shows that all organizations have problems formulating consent texts in an informative way, which is required for adequate data protection. Organizations also see challenges in the processing of personal data. These challenges consist of complex IT systems containing amounts of personal data that today cannot be managed in accordance with the Data Protection Regulation, as relevant system support is lacking.

## **Keywords**

GDPR, General Data Protection Regulation, Consent, Privacy policy

## **Förord**

Denna studie innefattar ett examensarbete inom ämnet för informatik. Studien har genomförts under kursen IK2017 (15 högskolepoäng) vid Systemvetenskapliga programmet på Högskolan Dalarna. Vi vill rikta ett tack till vår handledare Johan Håkansson samt alla informanter som gjort denna studie möjlig.

*Borlänge, 22 Maj 2018*

Two handwritten signatures in black ink. The first signature on the left is written in a cursive style and appears to be 'Teresa Olsson'. The second signature on the right is also cursive and appears to be 'Johan Håkansson'.

# Innehållsförteckning

1 Inledning .....	1
1.1 Bakgrund .....	1
1.2 Problemformulering .....	1
1.3 Syfte .....	1
1.4 Frågeställningar .....	2
1.5 Avgränsningar .....	2
2 Teoretisk referensram .....	3
2.1 Begreppslista .....	3
2.2 Personuppgiftslagen .....	3
2.3 Dataskyddsförordningen .....	4
2.4 Skillnaderna mellan PuL och GDPR .....	4
2.4.1 Konsekvensbedömning .....	4
2.4.2 Inbyggd integritet .....	4
2.4.3 Anmälan om personuppgiftsincident .....	4
2.4.4 Dataskyddsombud .....	5
2.4.5 Sanktionsavgift .....	5
2.4.6 Missbruksregeln försvinner .....	5
2.4.7 Ändamålsbegränsning .....	5
2.4.8 Information till den registrerade .....	5
2.4.9 Personuppgiftsansvarig och personuppgiftsbiträde .....	6
2.4.10 Dataskydd .....	6
2.4.11 Registerutdrag .....	6
2.4.12 Personuppgiftsincidenter .....	6
2.4.13 Datainspektionens roll .....	6
2.5 Rättslig grund för personuppgiftsbehandling enligt dataskyddsförordningen .....	6
2.6 Samtycke i enlighet med dataskyddsförordningen .....	7
2.6.1 Behandling av personuppgifter .....	8
2.6.2 Information vid registrering .....	8
2.6.3 Återkalla samtycke .....	8
2.7 Avslutande reflektion .....	8
3 Metod .....	10
3.1 Genomförande .....	10
3.2 Strategi .....	11
3.3 Litteraturstudie .....	12
3.4 Dokumentstudie .....	13
3.5 Intervjuer .....	14
3.6 Urval .....	15
3.7 Dataanalys .....	15
3.8 Metoddiskussion .....	15
4 Empiri .....	17
4.1 Presentation av organisationerna .....	17
4.2 Landstinget .....	17
4.2.1 Samtycke och samtyckestexter .....	17
4.2.2 Behandling av personuppgifter .....	18
4.3 Kommunen .....	19
4.3.1 Samtycke och samtyckestexter .....	20
4.3.2 Behandling av personuppgifter .....	20
4.4 Bostadsbolaget .....	21
4.4.1 Samtycke och samtyckestexter .....	22
4.4.2 Behandling av personuppgifter .....	22
4.5 Banken .....	23

4.5.1 Samtycke och samtyckestexter .....	23
4.5.2 Behandling av personuppgifter .....	24
5 Analys .....	25
5.1 Organisationernas samtyckestexter enligt dataskyddsförordningen .....	25
5.1.1 Landstinget .....	25
5.1.2 Kommunen .....	26
5.1.3 Bostadsbolaget .....	27
5.1.4 Banken .....	27
5.1.5 Skillnader och likheter mellan organisationerna .....	28
5.2 Organisationernas behandling av personuppgifter enligt dataskyddsförordningen .....	28
5.2.1 Landstinget .....	29
5.2.2 Kommunen .....	30
5.2.3 Bostadsbolaget .....	31
5.2.4 Banken .....	31
5.2.5 Skillnader och likheter mellan organisationerna .....	32
6 Diskussion .....	33
6.1 Organisationernas samtyckestexter enligt dataskyddsförordningen .....	33
6.2 Organisationernas behandling av personuppgifter enligt dataskyddsförordningen .....	34
7 Slutsatser .....	36
7.1 Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att utforma samtyckestexter i enlighet med dataskyddsförordningen? .....	36
7.2 Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att följa dataskyddsförordningen gällande personuppgiftsbehandlingen? .....	36
7.3 Kunskapsbidrag .....	36
7.4 Förslag på vidare forskning .....	37
8 Epilog .....	38
Källförteckning .....	39
Bilagor .....	41
Bilaga 1 – Intervjuguide .....	41
Bilaga 2 - Informationsbrev till intervjuperson .....	42
Bilaga 3 - Blankett för Etikprovning .....	43

## Figurförteckning

Figur 1: Forskningsprocessen (Oates, 2006) .....	11
Figur 2: Sökresultat på Datainspektionens webbplats .....	14

## Tabellförteckning

Tabell 1: Begreppslista .....	3
Tabell 2: Frågeställningar och frågeguide .....	9
Tabell 3: Söktabell – redovisning av data vid litteratursökning .....	13
Tabell 5: Organisationerna som studien innefattar .....	17
Tabell 6: Organisationernas utmaningar och åtgärder gällande samtyckestexter .....	25
Tabell 7: Organisationernas utmaningar och åtgärder gällande behandlingen av personuppgifter .....	29

# 1 Inledning

*Detta kapitel innefattar studiens bakgrund, problemformulering, syfte och frågeställningar samt avgränsningar.*

## 1.1 Bakgrund

Insamling av data har ökat väsentligt under de senaste decennierna (Gilmore, 2016). Dagens e-tjänster bygger till största del på individspecifika användardata vilket resulterat i att nya förhållningssätt krävs för att skydda den personliga integriteten (Rotenberg & Jacobs, 2013). Därför har nya lagstiftningar framtvingsats (ibid.). Europaparlamentet har tagit fram en ny förordning vid namn ”General Data Protection Regulation (GDPR)” eller på svenska ”dataskyddsförordningen” (Datainspektionen, 2017). Syftet med denna förordning är att skydda individers grundläggande rättigheter och friheter gällande personuppgiftsbehandlingen. Förordningen träder i kraft den 25 maj 2018 och ska då tillämpas i svensk lagstiftning. Ett annat syfte med förordningen är att harmonisera lagstiftningar angående behandlingen av personuppgifter inom hela EU (ibid.).

Det är varierande hur långt organisationer har kommit i omställningen till dataskyddsförordningen (Malmqvist, 2018, 9 april). Det är många företag som känner till dataskyddsförordningen men som ännu inte vidtagit åtgärder. I Europa är 75 procent av småföretagen och över 90 procent av medelstora företag medvetna om dataskyddsförordningen men enbart hälften av dem har påbörjat anpassningen (ibid.).

I Sverige kommer personuppgiftslagen (PuL) att ersättas av dataskyddsförordningen där Datainspektionen (2017) kommer att fungera som tillsynsmyndighet. Det finns en del tillägg och förändringar i dataskyddsförordningen som organisationer bör beakta. Organisationer måste tillhandahålla den registrerade relevant information rörande behandlingen av personuppgifter. Organisationer måste även se till att personuppgifter inte behandlas i onödan (ibid.).

Vid införandet av dataskyddsförordningen kommer organisationers samtyckestexter enligt personuppgiftslagen att behöva förändras för att stå i harmoni med förordningens regler (Datainspektionen, 2017). Andra omställningar som kan komma att behöva genomföras är organisationers IT-system då dataskyddsförordningen ställer högre krav på hur personuppgifter behandlas (ibid.). Denna studie kommer att presentera fyra organisationers utmaningar och omställningar gällande dataskyddsförordningen.

## 1.2 Problemformulering

Som tidigare nämnts införs dataskyddsförordningen den 25 maj (2018) och många företag har ännu inte påbörjat anpassningen för att leva upp till dess regler (Malmqvist, 2018, 9 april). Det kommer att ställas större krav för hur organisationer hanterar personuppgifter (Datainspektionen, 2017). Datainspektionen kommer att kunna utdöma en sanktionsavgift till den som inte lever upp till dataskyddsförordningens regler. Då dataskyddsförordningen ännu inte trätt i kraft finns det inga fall som kan påvisa hur detta kommer att tillämpas i praktiken (ibid.).

## 1.3 Syfte

Syftet med studien är att identifiera vilka åtgärder organisationer vidtagit för att följa dataskyddsförordningens regler och vilka utmaningar som kan uppstå i omställningen.

## 1.4 Frågeställningar

Utifrån beskrivet syfte och problemformulering ska den här studien ge svar på följande frågeställningar:

- Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att utforma samtyckestexter i enlighet med dataskyddsförordningen?
- Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att följa dataskyddsförordningen gällande personuppgiftsbehandlingen?

## 1.5 Avgränsningar

Vi har valt att avgränsa oss till organisationer i Sverige som behandlar personuppgifter. Denna avgränsning har genomförts för att beakta organisationer i en svensk kontext. Vi har valt fyra olika organisationer för att avgränsa omfattningen av studien. Vi har även valt att avgränsa oss till den privata- och offentliga sektorn.

Som kan ses i frågeställningarna avgränsas studien till samtyckestexter och behandlingen av personuppgifter samt hur organisationerna tillämpar dessa i praktiken. Denna avgränsning har gjorts då dataskyddsförordningen är omfattande.



## 2 Teoretisk referensram

*I detta kapitel presenteras kunskap om befintlig teori. Kapitlet har genererats utifrån litteratur och dokument rörande personuppgiftslagen och dataskyddsförordningen.*

### 2.1 Begreppslista

Här nedan (Tabell 1) presenteras studiens centrala begrepp samt dess innebörd. Syftet med denna begreppslista är att ge läsaren bredare kunskap i ämnet. Begreppslistan används även för att definiera hur begreppen används i den här studien.

<b>Samtyckestext</b> I denna studie används begreppet "samtyckestext". En samtyckestext är den text som innehåller information om personuppgiftsbehandlingen vid inhämtande av samtycke.
<b>Den registrerade</b> "Den som en personuppgift avser" (Personuppgiftslagen). "Den registrerade" i den här studien innefattar därmed den person vars personuppgifter behandlas. Den registrerade kan många gånger i tal vara synonymt med "användare" av en tjänst.
<b>Behandlas</b> Begreppet "behandlas" eller "behandling" är brett vilket i lagen innefattar: insamling, registrering, lagring, bearbetning, spridning med mera (Personuppgiftslagen).
<b>Samtycke (Eng. Consent)</b> Enligt skäl 32 (Europaparlamentets och rådets förordning (EU) 2016/679) är "samtycke" något den registrerade ska lämna åt den som kommer att behandla personuppgifterna. Samtycke ett avtal som den registrerade godkänner, detta genom en skriftlig, inklusive elektronisk, eller en muntlig förklaring (ibid.). "Samtycke" kan i tal vara synonymt med "medgivande".
<b>Uppfylla (Eng. Compliance)</b> I den här studien används begreppet "uppfylla" vilket syftar till att den som behandlar personuppgifter följer dataskyddsförordningens regler.

*Tabell 1: Begreppslista*

### 2.2 Personuppgiftslagen

Personuppgiftslagen (1998:204) förkortas och kallas ofta PuL (Datainspektionen, u.å.). Datainspektionen är tillsynsmyndigheten för personuppgiftslagen i Sverige. 1998 kom personuppgiftslagen att träda i kraft, lagen syftar till att skydda den personliga integriteten. Personuppgiftslagen bygger på beslut från EU:s dataskyddsdirektiv. Personuppgiftslagen innehåller bland annat samtycke och information till den registrerade. Samtycke är ett godkännande från den registrerade. Företag, myndigheter och föreningar kan utse ett personuppgiftsombud som har i uppgift att kontrollera att personuppgifter behandlas i enlighet med lagen. I personuppgiftslagen används termen "den/de registrerade" vilket innefattar den person vars personuppgifter behandlas av ett företag, en organisation eller en förening. En personuppgift innefattar all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Personuppgifter delas in i två kategorier vilka är strukturerade och ostrukturerade. Strukturerade personuppgifter kan vara om den registrerades personuppgifter sammanställs i ett register. Ostrukturerade personuppgifter kan vara om den registrerades personuppgifter används i exempelvis löpande text (ibid.).

## 2.3 Dataskyddsförordningen

Dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) nr 2016/679) kommer att börja gälla som lag den 25 maj 2018 i alla EU:s medlemsstater. I Sverige ersätts personuppgiftslagen med dataskyddsförordningen där Datainspektionen fortsatt ska fungera som tillsynsmyndighet (Datainspektionen, 2017). Dataskyddsförordningen även kallad GDPR står för ”General Data Protection Regulation” och kommer i Sverige att kompletteras med den svenska dataskyddslagen. Syftet med den nya dataskyddsförordningen är att skydda människors grundläggande rättigheter och friheter. Syftet är också att harmonisera behandlingen av personuppgifter inom EU. Ett annat syfte med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 då det digitala samhället nått nya höjder och lagen har på så sätt släpat efter (ibid.).

## 2.4 Skillnaderna mellan PuL och GDPR

Datainspektionen (2017) skriver på sin webbplats att mycket av reglerna i dataskyddsförordningen liknar personuppgiftslagen. Det finns dock några viktiga skillnader att beakta vid behandling av personuppgifter. Dataskyddsförordningens viktiga nyheter presenteras i kommande stycken.

### 2.4.1 Konsekvensbedömning

Innan varje planerad personuppgiftsbehandling som kan innebära särskilda risker för den registrerade ska det göras en bedömning (Datainspektionen, 2017). Denna bedömning innefattar vilka konsekvenser behandlingen kan få samt vilka åtgärder som måste vidtas för att minimera riskerna (Artikel 35, Europaparlamentets och rådets förordning (EU) 2016/679). I skäl 84 (ibid.) står det att personuppgiftsansvarige ska vara ansvarig för att en konsekvensbedömning utförs avseende dataskydd, framförallt genom att bedöma riskens ursprung, art, särdrag och allvar. Konsekvensbedömning fungerar inte på samma sätt enligt personuppgiftslagen. Citat enligt 31 § (PuL): *”Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas”*.

### 2.4.2 Inbyggd integritet

Enligt principen inbyggd integritet så bör man vidta åtgärder för att säkerställa dataskydd vid utveckling av tekniska IT-system (Datainspektionen, 2017). Åtgärderna gällande integritetsaspekterna bör vidtas i ett så tidigt skede som möjligt för att undvika kostnader och svårigheter. Vägledande principer vid utveckling av IT-system är uppgiftsminimering, lagringsminimering och pseudonymisering. Uppgiftsminimering används för att undvika den personuppgiftsbehandling som inte behövs. Lagringsminimering används i avseende att inte behandla personuppgifter som inte är ändamålsenliga. Pseudonymisering används som en åtgärd i avsikt att uppfylla kravet på uppgiftsminimering och inbyggd integritet. Anonymisering är en relevant åtgärd i avsikt att uppfylla kravet på lagringsminimering (ibid.).

### 2.4.3 Anmälan om personuppgiftsincident

Om ett dataintrång inträffar eller annan säkerhetsincident som förlust av personuppgifter ska det anmälas till Datainspektionen inom 72 timmar (Datainspektionen, 2017). Detta ska leda till att den registrerade informeras (ibid.). Citat ur skäl 85 (Europaparlamentets och rådets förordning (EU) 2016/679) *”Om en sådan anmälan inte kan ske inom 72 timmar, bör skälen till fördröjningen åtfölja anmälan och information får lämnas i omgångar utan otillbörligt vidare dröjsmål”*. Datainspektionen kommer att tillhandahålla en e-tjänst när dataskyddsförordningen träder i kraft (Datainspektionen, 2017). Denna e-tjänst kommer

att vara webbaserad och finnas tillgänglig på datainspektionens webbplats. E-tjänstens syfte är att förenkla inrapporteringen av personuppgiftsincidenter för den som behandlar personuppgifter (ibid.).

#### **2.4.4 Dataskyddsombud**

Om en organisation eller myndighet behandlar känsliga uppgifter eller uppgifter som kan innebära kartläggning av individers beteende måste det utses ett dataskyddsombud som bevakar dessa dataskyddsfrågor (Datainspektionen, 2017). Dataskyddsombudet ska på ett oberoende sätt kunna fullgöra sitt uppdrag (Skäl 97, Europaparlamentets och rådets förordning (EU) 2016/679). I personuppgiftslagen finns det ingen paragraf som behandlar ”Dataskyddsombud”.

#### **2.4.5 Sanktionsavgift**

Datainspektionen kommer att utdöma en sanktionsavgift för den som bryter mot förordningens regler. Det som kommer att beaktas är hur allvarlig överträdelsen är samt om det skett i avsiktligt eller oavsiktligt syfte (Datainspektionen, 2017). 20 miljoner Euro eller fyra procent av bolagets globala omsättning är den högsta avgiften som kan utdömas. Vid mindre allvarliga händelser kan två procent av bolagets globala omsättning utdömas (ibid.). Sanktionsavgifter förekommer ej i personuppgiftslagen (PuL). Dock kan skadestånd förekomma. Enligt 48 § (PuL) ska personuppgiftsansvarige ersätta den registrerade om kränkning av den personliga integriteten förekommit vid behandlingen.

#### **2.4.6 Missbruksregeln försvinner**

Personuppgiftslagen innefattas av missbruksregeln, denna regel kommer i dataskyddsförordningen att försvinna (Datainspektionen, 2017). Detta innebär att personuppgifter ska behandlas på samma sätt oavsett om dessa är strukturerade eller ostrukturerade (ibid.). Enligt Personuppgiftslagen behandlas strukturerade och ostrukturerade personuppgifter på olika sätt, detta kommer nu att upphöra när dataskyddsförordningen träder i kraft.

#### **2.4.7 Ändamålsbegränsning**

Behandling av personuppgifter får endast bedrivas förenligt med ändamålet. Personuppgiftsansvarige ska innan behandling av personuppgifter ansvara för och förstå ändamålet med behandlingen. Detta är ett tillägg i dataskyddsförordningen enligt regeln om ansvarsskyldighet (Artikel 5, Europaparlamentets och rådets förordning (EU) 2016/679). Detta innebär således att ingen annan behandling får utövas än den som uppgivits vid insamling. ”*De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål*”.

#### **2.4.8 Information till den registrerade**

I dataskyddsförordningen kommer ett större ansvar ligga hos den personuppgiftsansvarige. Ansvaret innefattar att kunna lämna information till den registrerade om hur dennes personuppgifter behandlas (Datainspektionen, 2017). Den registrerade ska även ha rätt till: rättelse, radering, begränsning av behandling samt kunna göra invändningar i hur personuppgifterna behandlas. Den registrerade ska kunna framföra sina klagomål till berörd organisation (ibid.). Enligt 23 § (PuL) ska den som behandlar uppgifter kunna lämna ut information om behandlingen till den registrerade. 25 § (PuL) förklarar punkterna för vad informationen ska innefatta. Dock är dessa punkter inte lika omfattande som i dataskyddsförordningen.

### **2.4.9 Personuppgiftsansvarig och personuppgiftsbiträde**

En nyhet i dataskyddförordningen är att många av de skyldigheter som tidigare har legat hos personuppgiftsansvarige också kommer att gälla för personuppgiftsbiträdet (Datainspektionen, 2017). Personuppgiftsansvarige är den som ansvarar för vilket ändamål personuppgifterna ska behandlas och hur behandlingen får utföras. Personuppgiftsbiträdet är den som behandlar personuppgifter åt personuppgiftsansvarige (ibid.).

### **2.4.10 Dataskydd**

I kommande och befintliga IT-system ska hänsyn tas till integritetsskyddsreglerna. Det finns ett krav på dataskydd som standard (privacy by default) i dataskyddsförordningen (Datainspektionen, 2017). Detta innebär att personuppgifter inte ska behandlas i onödan. Denna regel är inte lika omfattande i personuppgiftslagen som i dataskyddsförordningen (ibid.).

### **2.4.11 Registerutdrag**

Den registrerade ska på begäran kunna få ett registerutdrag om dennes personuppgifter (Datainspektionen, 2017). Registerutdraget ska innehålla information om var uppgifterna har insamlats, för vilket ändamål behandlingen utförs samt vilka som får ta del av dessa uppgifter. Registerutdraget ska lämnas i skriftlig form till den registrerade. Detta är ingen nyhet utan har sedan tidigare tillämpats i personuppgiftslagen (ibid.).

### **2.4.12 Personuppgiftsincidenter**

En skyldighet i dataskyddförordningen är att organisationer ska ha rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter (Datainspektionen, 2017). Denna regel är en nyhet och finns inte med i personuppgiftslagen (ibid.).

### **2.4.13 Datainspektionens roll**

I varje EU-land ska det finnas en tillsynsmyndighet som övervakar att dataskyddsförordningen följs. I Sverige är det Datainspektionen som har denna uppgift (Datainspektion, 2017). En nyhet i dataskyddsförordningen är att Datainspektionen kan utöva tillsyn mot både personuppgiftsansvariga och personuppgiftsbiträden (ibid.). Enligt personuppgiftslagen är det personuppgiftsansvarige som har ansvaret för behandlingen av personuppgifter. Under 2018 kommer Dataskyddsförordningen att byta namn till Integritetsskyddsmyndigheten.

## **2.5 Rättslig grund för personuppgiftsbehandling enligt dataskyddsförordningen**

För att följa dataskyddsförordningens regler krävs det att den organisation som behandlar personuppgifter har en rättslig grund för ändamålet med behandlingen (Datainspektionen, 2017). Dataskyddsförordningen innehåller olika rättsliga grunder för behandling vilka är; avtal, intressevägning, rättslig förpliktelse, myndighetsutövning och uppgift av allmänt intresse, grundläggande intresse samt samtycke. Avtal innefattar att den registrerade har eller ska ingå ett avtal med den personuppgiftsansvarige. Intresseavvägning används om personuppgiftsansvarige har ett intresse som väger tyngre än den registrerades, denna behandling kan då ske utan samtycke. Rättslig förpliktelse innefattar att personuppgiftsansvarig har skyldighet ur annan lag att behandla personuppgifter som ett led i sin verksamhet. Personuppgifter kan behöva behandlas genom myndighetsutövning eller om uppgifterna behöver behandlas av allmänt intresse. Grundläggande intresse

innefattar att personuppgifter får behandlas om den registrerade inte kan lämna sitt samtycke under specifika omständigheter (exempelvis vid medvetlöshet). Slutligen används samtycke som en sista utväg att stödja sig emot om personuppgiftsansvarige inte kan hitta annan rättslig grund för behandlingen. För att personuppgiftsbehandlingen ska vara laglig krävs någon av de ovanstående rättsliga grunderna (ibid.).

## 2.6 Samtycke i enlighet med dataskyddsförordningen

Grunden för att personuppgifter ska få behandlas är att den som behandlar uppgifterna har ett samtycke från den registrerade om ingen annan rättslig grund finns (Datainspektionen, 2017). Ett samtycke ska vara frivilligt samt att den registrerade fått information om vad behandlingen kommer att innefatta (ibid.). Bhaimia (2018) förklarar att dataskyddsförordningen kommer att ställa högre krav på att den som behandlar personuppgifter kan visa upp en laglig grund gällande behandlingen för den registrerade.

När dataskyddsförordningen träder i kraft kommer det att ske förändringar i hur inhämtning av personuppgifter ska se ut och på vilket sätt organisationerna inhämtar samtycke (Appelgren, 2017). Användarna kommer enligt Appelgren att få en djupare förståelse för hur och vilka personuppgifter som behandlas. När dataskyddsförordningen träder i kraft ska det i praktiken innebära att gapet mellan företag och användare kommer att minska. Användare kommer att få större kunskap om i vilken utsträckning de ”övervakas” samt vilken data som inhämtas och i vilket syfte. Dataskyddsförordningen kommer troligtvis öka användarnas medvetenhet (ibid.).

Jørgensen och Desai (2017) förklarar att brister som tidigare funnits i samtycken förbättras med hjälp av dataskyddsförordningens nya regler. Jørgensen och Desai menar också att den registrerade har rätt till lättillgänglig information då den registrerade måste lämna samtycke samt vara införstådd med vad villkoren innefattar. Organisationer kan inte längre gömma sig bakom samtyckestexter som den registrerade inte förstår. Det återstår att se om den registrerade avslutar olika medlemskap genom att inte ge sitt samtycke till behandlingen av personuppgifter. Jørgensen och Desai ifrågasätter om ett samtycke kan ses som fritt ifall den registrerade lämnat sitt samtycke trots att han eller hon endast vill använda en begränsad del av en tjänst. Ett exempel på detta är Facebook som tillhandahåller flertalet tjänster under samma plattform (ibid.).

### **Informativt samtycke**

Det har under en längre tid diskuterats hur det på bästa sätt ska vara möjligt att skydda de registrerades personuppgifter menar Noain-Sánchez (2016). Vilka personuppgifter som kan uppfattas vara känsliga kan i flera avseenden vara ett individuellt subjektivt antagande. Därav bör det vara den registrerade själv som värdesätter sina personuppgifter och i vilken utsträckning han eller hon vill dela med sig av sina personuppgifter. Organisationen som ska behandla den registrerades data bör sträva efter att formulera en samtyckestext som ska vara så informativt som möjligt. Genom en informativ samtycketext ska den registrerade förstå vilka konsekvenser behandlingen kan innefatta. Den registrerade ska ges möjlighet att värdesätta sina personuppgifter innan behandlingen (ibid.).

Syftet med dataskyddsförordningen är att de registrerades personuppgifter skall skyddas och att dess integritet ska värdesättas (Noain-Sánchez, 2016). I skapandet av ett informativt samtycke menar Noain-Sánchez att integriteten bör upprätthållas även innan behandlingen kommer att ske. Genom tillräckligt med information till den registrerade ska denne kunna fatta beslut om att lämna samtycke. Detta ska bidra till en känsla av självständighet och integritet. Det är av yttersta vikt att användaren redan innan lämnat

samtycke bör få en förståelse för vilka negativa och oönskade konsekvenser som kan uppstå vid behandlingen. Detta ansvar ligger hos organisationen som ansvarar för behandlingen av personuppgifter och samtyckestextens utformning (ibid.). Enligt Zuiderveen & Poort (2017) har det visat sig att den registrerade sällan uppfattar vad dennes personuppgifter kommer att användas till.

### **2.6.1 Behandling av personuppgifter**

Enligt artikel 6 (Europaparlamentets och rådets förordning (EU) 2016/679) är behandlingen endast laglig om någon av följande villkor är uppfyllda: den registrerade har lämnat samtycke, fullgöra avtal med den registrerade, fullgöra rättslig förpliktelse, skydda intressen för den registrerade eller annan fysisk person, uppfylla uppgift av allmänt intresse, led i myndighetsutövning. Det är upp till varje medlemsland att införa mer specifika bestämmelser (ibid.).

### **2.6.2 Information vid registrering**

Vid samtycke enligt artikel 7 (Europaparlamentets och rådets förordning (EU) 2016/679) ska personuppgiftsansvarige på ett tydligt sätt visa den registrerade att han eller hon samtyckt. Den registrerade ska på ett tydligt sätt förstå vad han eller hon har samtyckt till, annars behöver inte samtycket vara bindande (ibid.).

### **2.6.3 Återkalla samtycke**

Framträdande i dataskyddsförordningen är att den registrerade med enkelhet och när som helst ska kunna återkalla sitt samtycke (European Parliament, 2017). När samtycke erhålls via elektroniska medel genom endast ett musklick, svep eller tangenttryckning måste den registrerade i praktiken kunna återkalla sitt samtycke lika lätt. Kravet på ett enkelt tillbakadragande beskrivs som en nödvändig aspekt av ett giltigt samtycke i dataskyddsförordningen (ibid.).

## **2.7 Avslutande reflektion**

Genom att jämföra personuppgiftslagen och dataskyddsförordningen formulerade vi en frågeguide i syfte att besvara studiens frågeställningar. För att besvara den första frågeställningen rörande samtyckestexter används frågeguidens (Bilaga 1) (Tabell 2) fråga 2, 3, 6 och 7. För att besvara den andra frågeställningen rörande behandlingen av personuppgifter används frågeguidens fråga 5. Fråga 5 används även för att besvara första frågeställningen rörande samtycke. Den första frågan i frågeguiden är en öppningsfråga som används för att förstå organisationernas attityd till dataskyddsförordningen. Den teoretiska referensramen har applicerats för att analysera studiens empiriska material. I analyskapitlet ställs det empiriska materialet mot befintlig litteratur som presenterats i detta kapitel.

Frågeställningar	Frågeguide
<ul style="list-style-type: none"> <li>• Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att utforma samtyckestexter i enlighet med dataskyddsförordningen?</li> <li>• Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att följa dataskyddsförordningen gällande personuppgiftsbehandlingen?</li> </ul>	<ol style="list-style-type: none"> <li>1. Hur ser ni på införandet av dataskyddsförordningen inom er organisation?</li> <li>2. Krävs det stora omställningar i era nuvarande samtyckestexter (enl. PuL) för att upprätthålla dataskyddsförordningens regler och vilka utmaningar ser ni i dessa omställningar?</li> <li>3. Krävs det stora omställningar i er nuvarande personuppgiftsbehandling (IT-system) för att upprätthålla dataskyddsförordningens regler och vilka utmaningar ser ni i dessa omställningar?</li> <li>4. Kommer ert syfte vid behandlingen av personuppgifter att förändras i omställningen till den nya dataskyddsförordningen och dess förändrade riktlinjer för samtycke?</li> <li>5. Kommer era nya samtyckestexter (enl. dataskyddsförordningen) att överensstämma med hur ni i praktiken kommer att behandla personuppgifter eller vilka åtgärder måste ni vidta för att dessa ska stämma överens?</li> <li>6. Vilka åtgärder har vidtagits vid framtagandet av samtyckestexter (enl. dataskyddsförordningen) för att det ska vara så informativt som möjligt för den registrerade?</li> <li>7. Är era nya samtyckestexter (enl. dataskyddsförordningen) tillräckligt informativa för att den registrerade ska kunna fatta ett avgörande beslut i fråga att ingå avtal?</li> </ol>

*Tabell 2: Frågeställningar och frågeguide.*

## 3 Metod

*I detta kapitel beskrivs studiens tillvägagångssätt vilket innefattar; genomförande, strategi, litteraturstudie, dokumentstudie, urval, intervjuer, dataanalys och metoddiskussion.*

### 3.1 Genomförande

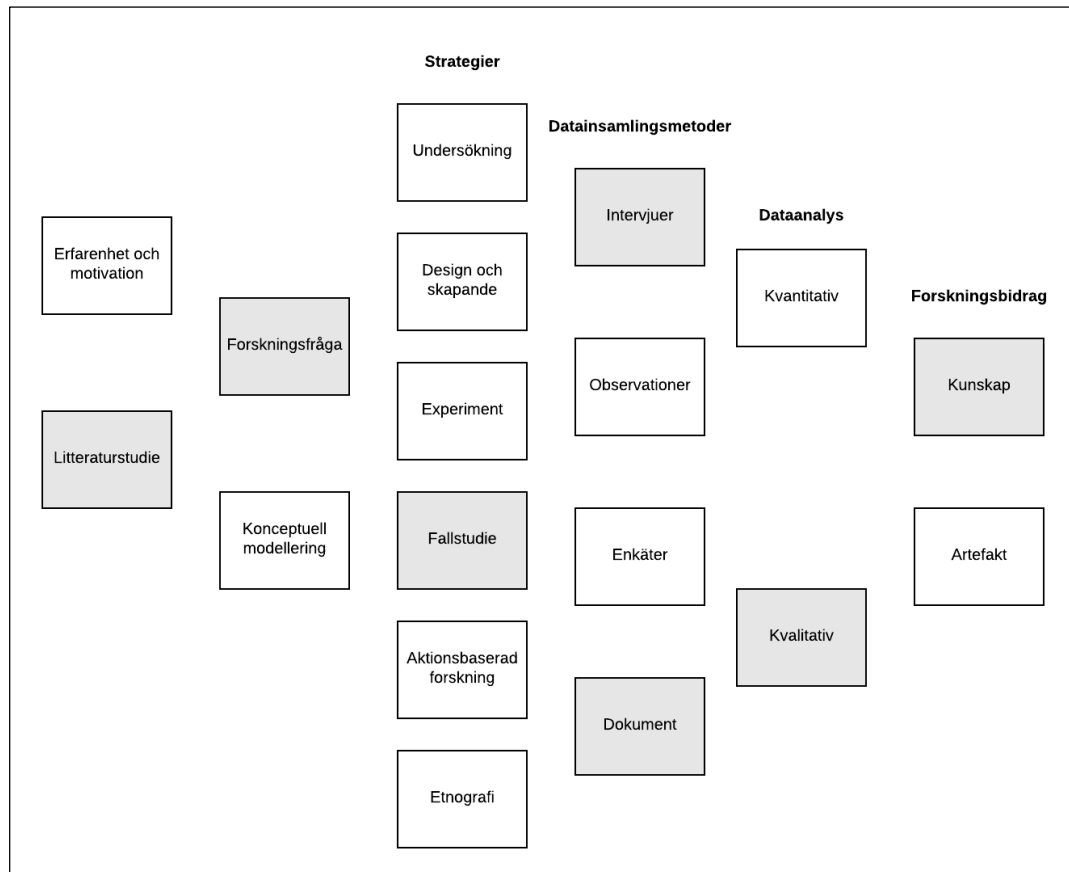
Vi började med att utforma ämnet som studien behandlar, det vill säga dataskyddsförordningen. Vi valde därefter att avgränsade oss till samtyckestexter och behandlingen av personuppgifter. Vi genomförde en litteraturstudie för att bygga upp en teoretisk referensram. Därefter utformade vi vårt syfte och våra frågeställningar samt började vi att skriva på introduktionskapitlet. Syftet och frågeställningarna omformulerades ett flertal gånger i början av arbetsgången med anledning att specificera ämnet. När studiens design utformades valde vi att intervjua ett antal organisationers företrädare i ämnet. Detta val gjordes för att vi skulle kunna undersöka hur dessa organisationer behandlar frågor rörande dataskyddsförordningen.

När introduktionskapitlet och den teoretiska referensramen påbörjats valde vi att utforma en intervjuguide (Bilaga 1). Under den tid som vi formulerade vår intervjuguide började vi också att leta efter informanter. Allt eftersom vi fick kontakt med informanterna bokade vi in tid och datum för intervjuerna. Efter genomförda intervjuer transkriberade vi materialet för att sedan kunna sammanfatta det viktigaste i empirikapitlet.

Vi skrev därefter en analys där det empiriska materialet analyserades mot den teoretiska referensramen. I diskussionskapitlet diskuterades det analyserade materialet. Vi har också en slutsats som ger svar på studiens frågeställningar. Slutligen presenterar vi ett kunskapsbidrag.

Nedan i Figur 1 illustreras forskningsprocessen enligt Oates (2006). De gråmarkerade rutorna är de steg i forskningsprocessen vi valt att använda oss av.





Figur 1: Forskningsprocessen (Oates, 2006)

### 3.2 Strategi

Vi har valt strategin fallstudie. En fallstudie karaktäriseras av att den studeras på djupet och innefattar varierande datainsamlingsmetoder (Oates, 2006). I denna studie har vi undersökt hur fyra organisationer ser på sina utmaningar gällande samtyckestexter och sin personuppgiftsbehandling för att vara förenliga med dataskyddsförordningen. För att identifiera utmaningar och åtgärder krävdes det att vi studerade dessa organisationer på djupet. Därav fann vi det lämpligt att använda oss av en fallstudie.

För att skapa en djupare förståelse i ämnet valde vi att genomföra både en litteraturstudie och en dokumentstudie. Litteraturstudien genomfördes för att studera vad tidigare forskning säger om ämnet. Dokumentstudien användes som ett komplement till litteraturstudien då den hjälpte oss att förstå hela ämnets kontext. I Dokumentstudien utgick vi från Datainspektionens material.

För att samla in studiens empiriska material använde vi oss av datainsamlingsmetoden intervjuer. Genom att använda intervjuer som metod har vi kunnat förstå organisationernas utmaningar och åtgärder som uppstått i omställningen till dataskyddsförordningen. Intervjuer är den datainsamlingsmetod som bäst skildrar personers olika utsagor (Oates, 2006). Detta anser vi är fördelaktigt i denna studie då syftet med intervjuerna var att i ett senare skede kunna redogöra för organisationers omställning till dataskyddsförordningen. Kritik som kan riktas mot datainsamlingsmetoden intervjuer i vårt fall är att endast en individ står som representant för varje enskild organisation.

Oates (2006) beskriver även ytterligare två datainsamlingsmetoder, observationer och enkäter. Observationer innefattar att forskaren observerar ett visst fenomen eller en händelse och sedan reflekterar över det inträffade (ibid.). Observationer har inte varit tillämpbara i denna studie då vi var tvungna att ställa frågor till informanterna för att generera den data som krävdes. Enkäter är fördefinierade frågor och innefattar förutbestämda svarsalternativ (Oates, 2006). Vi valde att inte använda oss av enkäter då det inte skulle generera den tänkta data vi var ute efter. Därav ansåg vi intervjuer var en bättre insamlingsmetod i det här fallet.

För att förhålla oss opartiskt vilket är viktigt i en studie av denna karaktär har vi inte samarbetat med någon av organisationerna.

### 3.3 Litteraturstudie

En litteraturstudie används för att undersöka och klargöra tidigare forskning inom aktuellt område (Oates, 2006). En litteraturstudie används också för att redovisa vad som tidigare konstaterats. Identifierad kunskap och information redovisas sedan för att stärka forskarens egna idéer och resonemang (ibid.)

Vi har utfört en litteraturstudie för att skapa oss kunskap i ämnet samt för att se vad tidigare forskning säger. Eftersom studien till stor del handlar om förordning och lagtext krävdes det att vi också hade kunskap om detta. För att genomföra litteratursökningar använde vi oss av Högskolan Dalarnas söktjänst Summon (söktjänst för bibliotekets tryckta och elektroniska material). För att hitta relevant material till vår studie använde vi oss av flera sökord i olika konstellationer vilket redovisas i Tabell 3. Vi har även valt att till största del filtrera sökningarna utifrån artiklar som är "peer review". "Peer review" (engelska) eller på svenska "referensgranskning" är ett granskningsförfarande som görs av forskare med liknande kompetens vilket har tillämpats som praxis sedan 1900-talet (Jerkert, u.å.). Ytterligare en filtrering som genomförts vid sökningarna var "full text". "Full text" används i databasen för att visa det fullständiga materialet från respektive artikel i textform.

Här nedan (Tabell 3) visas en tabell med data för vilka litteratursökningar som genomförts. Tabellen innehåller data om artikelns namn, vem som författat artikelns, vilken databas sökningen är genomförd i, vilka sökord som används, vilket datum artikeln är hämtad, antalet träffar vid aktuell sökning samt vilka avgränsningar som hjälpt till att begränsa sökresultatet.

Artiklens namn	Författare	Databas	Sökord	Hämtad	Träffar	Avgränsningar
The reasons behind tracing audience behavior	Appelgren, E	Summon	consent cookies gdpr	2018-04-09	23	Fulltext, Peer-Review
Online price discrimination and EU data privacy law	Zuiderveen Borgesius, F., & Poort, J	Summon	consent cookies gdpr	2018-04-09	23	Fulltext, Peer-Review
The general data protection regulation	Bhaimia, S	Summon	gdpr consent	2018-04-10	110	Fulltext, Peer-Review
Right to privacy meets online platforms	Jørgensen, R. F., & Desai, T	Summon	gdpr it-system	2018-04-10	131	Fulltext, Peer-Review
GDPR - A Y2K-II for business?	Bihari, E	Summon	gdpr it-system	2018-04-10	131	Fulltext, Peer-Review
Updating the law of information privacy	Rotenberg, M., & Jacobs, D	Summon	gdpr it-system	2018-04-10	131	Fulltext, Peer-Review
“Privacy by default” and active “informed consent” by layers	Amaya Noain-Sánchez	Summon	gdpr consent cookies	2018-04-10	23	Fulltext, Peer-Review
“Can obtaining informed consent alter self-reported drinking behaviour? A methodological experiment”	Lambert Felix, Patrick Keating and Jim McCambridge	Summon	data consent behaviour	2018-04-11	567 971	Fulltext, Peer-Review

Tabell 3: Söktabel – redovisning av data vid litteratursökning.

### 3.4 Dokumentstudie

Dokumentstudier kan vara ett annat sätt att hitta relevant data utöver intervjuer och observationer (Oates, 2006). Vi valde att komplettera vår litteraturstudie med hjälp av en dokumentstudie. Materialet som framkom i dokumentstudien presenteras i kapitlet för teoretisk referensram. Vi har presenterat insamlat materialet under teoretisk referensram istället för under empiri då vi anser att det kompletterar litteraturstudien.

Vid dokumentstudier är det viktigt att skapa sig en objektiv bild av dokumenten som studeras (Patel & Davidson, 2003). Det är också viktigt att vara källkritisk för att kunna avgöra hur trovärdigt materialet är (ibid.). Då Datainspektionen är tillsynsmyndigheten för dataskyddsförordningen anser vi att dokument och artiklar från dess webbplats kan anses innehålla trovärdig information. Dokumentstudierna innefattar således information om dataskyddsförordningen och personuppgiftslagen.

I löpande text anges inte Datainspektionen (2017) med någon bokstav som definierar vilken artikel det rör sig om. Källförteckningen innehåller således inte heller någon information om vilka artiklar vi använt oss av från Datainspektionens webbplats. Detta har att göra med att Datainspektionen gjort om sin webbplats under studiens gång. Besökaren blir endast skickad till sidan som övergripande behandlar dataskyddsförordningen, detta om en föråldrad URL (Uniform Resource Locator) används. För att läsa vidare om problematiken med Datainspektionens webbplats se artikel: ”Datainspektionens jätteblunder: det går inte längre att hitta GDPR-informationen” (Koskelainen, (2018, 23 maj). För att lösa denna problematiken vid kontroll av källor rekommenderar vi läsaren att använda sig av sökfältet på Datainspektionens webbplats (Se exemplet i Figur 2). Vid sök på ett begrepp kommer informationen tydligt upp i sökresultatet. Vi beklagar att detta har ställt till med problem för läsaren men vi hoppas att detta ska hjälpa till vid kontroll av källor.

The screenshot shows the website for Datainspektionen. At the top left is the logo and name. To the right are navigation links: OM OSS, KONTAKTA OSS, PRESS, A-Ö, and OTHER LANGUAGES. Below these is a search bar with the text 'Sök frågor och svar, vägledning och regler...' and a magnifying glass icon. A dark red navigation bar contains the following menu items: OM INTEGRITET, VÄGLEDNINGAR, LAGAR & REGLER, and KURSER & FÖRELÄSNINGAR. Below this bar, there is a breadcrumb trail 'Start → Sök' and another search bar with the text 'Personuppgiftsbiträdet' and a magnifying glass icon. The main heading is 'Sökresultat'. Below the heading, it says 'Din sökning på "personuppgiftsansvarige" gav 39 träffar'. The first result is titled 'Personuppgiftsbiträdets skyldigheter' and the text below it reads: 'Personuppgiftsbiträdets skyldigheter Den personuppgiftsansvarige har alltid det huvudsakliga ansvaret för ... är ni skyldiga att rapportera till den personuppgiftsansvarige om ni upptäcker en personuppgiftsincident'.

Figur 2: Sökresultat på Datainspektionens webbplats

### 3.5 Intervjuer

Då vi valde att göra en fallstudie av kvalitativ karaktär bestämde vi oss för att samla in data genom intervjuer. Intervjuerna som genomfördes var av intervjutypen semistrukturerade intervjuer. Att använda sig av semistrukturerade intervjuer innefattar att intervjuledaren har färdiga frågor men är beredd att byta ordningsföljd och/eller ställa följdfrågor (Oates, 2006). Följdfrågor kan användas för att skapa ett utvecklat resonemang (ibid.).

När vi formulerade intervjufrågorna (Bilaga 1) var tanken att dessa skulle kunna besvara vårt syfte och våra frågeställningar. Det var också meningen att ge utrymme för följdfrågor om det krävdes för att samla in den data vi var ute efter. Oates (2006) menar att följdfrågor är ett bra alternativ att använda sig av för att samla in den data forskaren söker. Frågorna formulerades utifrån förordningens regler och på så sätt kunde vi jämföra och se om organisationerna vidtagit relevanta åtgärder.

I god tid före varje intervju fick informanterna ta del av vårt informationsbrev (Bilaga 2). Informationsbrevet innehåller bland annat syftet med studien, vilken kunskap studien förväntas ge samt etiska aspekter. Informanterna fick därefter ta ställning till informationen om de ville delta i studien, detta gjordes genom ett muntligt samtycke.

Intervjuerna antecknades till viss del. För att underlätta och komplettera anteckningarna valde vi också att spela in intervjuerna med hjälp av inspelningsutrustning. Att spela in en intervju är ett bra sätt att dokumentera hela intervjumaterialet (Oates, 2006). Eftersom informanter kan bli nervösa och/eller kanske inte gillar att bli inspelade frågade vi varje informant om det var okej.

För att på ett enklare sätt få en tydligare bild av intervjuerna är det bra att transkribera det inspelade materialet (Oates, 2006). Vi valde att transkribera intervjumaterialet då vi ansåg att det var fördelaktigt i dataanalysen.

### 3.6 Urval

Ett kriterium för informanterna i denna studie var att de kunde svara på frågor gällande samtyckestexter och personuppgiftsbehandling. Då vi ville ha svar på detta var det lämpligt att intervjua personer med en befattning inom IT eller verksamhetsutveckling alternativt ett dataskyddsbud. Subjektivt urval är ett icke slumpmässigt urval och innefattar att forskaren handplockar informanter (Oates, 2006). Vi valde att utföra ett selektivt urval av informanter baserat på de befattningar vi trodde skulle kunna besvara vår frågeguide.

Vi kontaktade individer med följande befattningar; dataskyddsbud, kommunjurist, extern jurist och IT-chef. Vi ansåg att dessa informanter skulle besitta tillräcklig med kunskap för att kunna besvara våra intervjufrågor. Vi valde att intervjua fyra informanter, en från respektive organisation. Hälften av informanterna representerar den offentliga sektorn och den andra hälften representerar den privata sektorn.

### 3.7 Dataanalys

Enligt Björklund och Paulsson (2003) innebär induktion att ett ämne kan studeras utan att forskaren läst in sig på existerande teori då det senare är möjligt att formulera teori utifrån det insamlade materialet. Vid deduktion börjar forskaren med att läsa in sig på befintliga teorier som sedan verifieras med det insamlade materialet. Om dessa två ansatser används tillsammans under studiens gång kallas detta för abduktion (ibid.).

Vårt förhållningssätt i den här studien var abduktion då vi använt oss av både induktion och deduktion. Vi studerade befintlig litteratur för att skapa oss kunskap i ämnet vilket är en deduktiv ansats. Efter genomförda intervjuer ansåg vi att vårt empiriska material krävde mer teori för att en analys skulle vara genomförbar. Vi valde då att fördjupa oss i teori för att söka svar i det empiriska materialet vilket är en induktiv ansats.

De två teman som analyserats är organisationernas utmaningar och åtgärder rörande samtyckestexter och behandlingen av personuppgifter. I analyskapitlet presenteras två tabeller, en angående samtyckestexter och en angående behandlingen av personuppgifter. Utifrån det insamlade materialet som presenteras i empirikapitlet har vi sammanfattat alla organisationers utmaningar och åtgärder. Dessa utmaningar och åtgärder presenteras i tabellerna. Tabellerna ska hjälpa läsaren att få en överblick för vilka utmaningar och åtgärder som finns inom respektive organisation. Tabellernas innehåll har formulerats på ett likartat sätt för att läsaren lättare ska kunna se ett mönster i vilka utmaningar och åtgärder som finns. För att analysera utmaningar och åtgärder har befintlig litteratur använts (deduktion) men det har även tillkommit vissa teoretiska kompletteringar (induktion) för att slutföra analysen. Genom att analysera det insamlade materialet på ovanstående vis har vi kunnat besvara studiens syfte och frågeställningar.

### 3.8 Metoddiskussion

Vi har under arbetets gång identifierat både svagheter och styrkor med studiens metod. En nackdel kan vara att denna studie genomfördes månaderna innan införandet av dataskyddsförordningen (2018-05-25). Vi förstod att många organisationer skulle vara upptagna av att behandla dessa frågor internt. Som vi misstänkte var det svårt att komma i kontakt med relevanta informanter inom valda organisationer och därför blev också antalet informanter begränsade. Det har också varit svårt att analysera vårt insamlade material då litteraturen för ämnet är väldigt begränsat då dataskyddsförordningen ännu inte trätt i kraft.

Det hade varit möjligt att komplettera fallstudien med kvantitativdata genom att en testgrupp läst samtyckestexter och fått utvärdera dessa i en enkät. Vi hade då kunnat mäta utifrån givna parametrar om samtyckestexterna uppfyller kravet för informativt samtycke. Detta hade kunnat komplettera och visa om organisationerna formulerat samtyckestexterna så att den registrerade (användaren) förstår hur dennes personuppgifter behandlas.

En svaghet med vår frågeguide kan vara att frågorna inte alltid uppfattades korrekt och vi blev då tvungna att omformulera och förklara frågan på nytt. Eftersom vi valt semistrukturerade frågor hade vi möjlighet till följdfrågor vilket gjorde att vi ändå kunde fånga upp det material vi sökte efter.

Informantens position var i tre av fyra fall ett dataskyddsbud. Att intervjua ett dataskyddsbud ser vi som positivt för studien då denne är insatta i dataskyddsfrågor. I intervjuerna med respektive dataskyddsbud ansåg vi att svaren verkligen representerar vad organisationen står för. Vid en av intervjuerna var informantens position IT-chef. Vi såg att den informanten hade svårare att svara på dataskyddsfrågor eftersom det inte ligger inom dennes huvudområde. Då svaren upplevdes som osäkrare kan vi därför inte värdera svaren lika högt i denna intervju som i de övriga tre intervjuerna. Vi anser att det hade varit bättre om samtliga intervjuer genomförts med ett dataskyddsbud. Anledningen till valet av IT-chefen var att hen själv ville ställa upp som representant för organisationen.

Då införandet av dataskyddsförordningen ännu inte trätt i kraft är litteraturen begränsad och bygger till största del på spekulationer vilket kan ses som en nackdel med studien. Dock hade vi kunnat göra djupare litteraturstudier kring personuppgiftslagen. Detta hade kunnat visa hur väl organisationer beaktat lagen och vilka domar som tidigare utdöms.

Istället för subjektivt urval hade vi kunnat använt oss av självselektionsurval. Självselektionsurval innefattar att forskaren annonserar sitt ämne och behovet av informanter (Oates, 2006). Informanterna får sedan anmäla sig om de själva känner att de har någonting att tillföra (ibid.). Med självselektionsurval hade vi kunnat skapa oss ett större utbud av informanter och på så sätt kunnat tagit del av en större mängd data. Det är viktigt att belysa att forskaren avgör vilken data som är relevant för studien.

Svårigheter med studien var att formulera intervjuguiden (Bilaga 1). Till en början hade vi svårigheter att formulera frågor som skulle kunna besvara våra frågeställningar. Intervjuguiden omformulerades ett antal gånger i början av studien och vi var osäkra på om dessa frågor skulle ge oss den data vi sökte. För att ta reda på om frågorna var välformulerade och hade rätt innehåll kunde vi istället genomföra en testintervju. Vi hade kunnat valt en testperson som var insatt i dessa frågor och på så sätt kunnat utvärdera om frågorna var relevanta i syfte att samla in den data vi sökte. Detta kan ses som kritik vilket vi kan ha i beaktning för framtida studier.

## 4 Empiri

*Kapitlet inleds med att presentera studiens informanter och dess tillhörande organisationer. Därefter presenteras en sammanställning av studiens genomförda intervjuer. Det ska förtydligas att intervjuerna har ägt rum ungefär en till två månader innan dataskyddsförordningens inträde.*

### 4.1 Presentation av organisationerna

För att anonymisera respektive organisation i den här studien har vi valt att kalla dessa för; Landstinget, Kommunen, Bostadsbolaget och Banken (Tabell 4). Landstinget är ett landsting i Sverige (offentlig verksamhet) där informantens arbetstitel är landstingsjurist och dataskyddsbud. Kommunen är en kommun i Sverige (offentlig verksamhet) där informantens arbetstitel är kommunjurist och dataskyddsbud. Bostadsbolaget är ett svenskt aktiebolag (privat verksamhet) som bedriver ett bostadsbolag där informantens arbetstitel är IT-chef. Banken är en svensk bank (privat verksamhet) som bedriver elektroniska betalningslösningar där informantens arbetstitel är extern jurist (dataskyddsbud).

Namn i studien	Organisation	Informantens position
Landstinget	Ett landsting i Sverige	Landstingsjurist (Dataskyddsbud)
Kommunen	En kommun i Sverige	Kommunjurist (Dataskyddsbud)
Bostadsbolaget	Ett svenskt bostadsbolag (AB)	IT-chef
Banken	En svensk bank	Extern jurist (Dataskyddsbud)

*Tabell 4: Organisationerna som studien innefattar.*

### 4.2 Landstinget

Organisationen har som huvudsaklig uppgift att bedriva offentligt finansierad hälso- och sjukvård. Organisationen har även i uppgift att bli en regional kollektivtrafikmyndighet. Personuppgifterna som behandlas i huvudsak är patientuppgifter inom hälso- och sjukvård. Organisationen ansvarar för journalsystem, personaladministrativa IT-system samt IT-system som behandlar och analyserar patientdata. Organisationen menar även att det finns många IT-system som är hemmasnickrade där personuppgifter inte behandlas i enlighet med dataskyddsförordningen.

Organisationen har en grupp som arbetat med frågor rörande dataskyddsförordningen sedan 2016. Det finns stora förvirringar i verksamheten då många tror att det krävs samtycke för all behandling av personuppgifter. Många i organisationen tror att personuppgifter inte får behandlas alls. Ett stort arbete har genomförts i att informera personal i organisationen om hur dataskyddsförordningen kommer att tillämpas.

#### 4.2.1 Samtycke och samtyckestexter

Organisationen anser att det inte är några markanta omställningar i samtyckestexterna som krävs då de ofta stödjer sig på annan rättslig grund.

*”Det vi använder samtycke för är oftast om de är bildpublicering med redaktionellt inslag och när vi gör marknadsföring och vill ta bilder på medarbetare som är med på bild, då har vi samtycke men även när vi publicerar vissa nyhetsartiklar på vår internwebb”.*

Organisationens största skillnad blir att vara mer tydlig i vad personuppgifterna kommer att användas till och vilka uppgifter som kommer att behandlas samt hur samtycke återkallas. För att underlätta processen har organisationen tankar om att ha en funktionsbrevlåda eller en avdelning att kontakta för att återkalla samtycke.

Organisationens tanke är att personuppgiftsbehandlingen ska stämma överens med vad som står i samtyckestexterna annars är de medvetna om att dataskyddsförordningen inte följs. För att få ett dokumenterat underlag har organisationen valt att samla in samtycke via samtyckesblanketter. Organisationens samtyckestexter är ännu inte klara men följande sägs:

*”Det som vi kommer göra är att vi kommer beskriva ändamålet för behandlingen. Det är viktigt att förklara för den enskilda, varför vi vill ha de här uppgifterna. Även vilka uppgifter det är vi samlar in. Dom två är dom viktigaste så man vet tydligt vad det är man samtycker till. En annan viktig sak när man samtycker är att inte får baka in samtycke i någonting annat”.*

Samtyckestexterna är under remiss och ännu inte publicerade, men de förväntas att publiceras före den 25:e maj (2018).

Vad som beaktats är att samtyckestexterna ska vara så informativa som möjligt och att samtycke ska lämnas i en aktiv handling. En annan aspekt är att samtyckestexten ska förstås av alla. Organisationen säger följande:

*”Inte längre ha dom här 20 sidorna juridisk text som förklarar personuppgiftsbehandlingen, utan det ska vara enkel text så att man kan förstå vad det är för behandling som kommer att äga rum, det har vi också försökt göra. Då får man beskriva ändamålet med insamlingen, vilka uppgifter det är och vem man kan kontakta om man har frågor om behandlingen, och hur man återkallar sitt samtycke”.*

Organisationen ska sträva efter att ge den registrerade valmöjligheter i form av ett ”smörgåsbord när man godkänner” samtycken. Med det menas att den registrerade inte ska behöva godkänna till allt utan endast delar som han eller hon känner är relevanta. Detta ska ske för att inte tvinga den registrerade att lämna uppgifter mot sin vilja.

Något annat som behöver justeras i samtyckestexterna är hur länge personuppgifterna kommer att behandlas. *”Det kan vara bra att tidsbegränsa hur länge man behöver behandla uppgifterna. Så att man inte behandla uppgifter i onödan fastän man har ett samtycke”.*

För att kunna anpassa sig till dataskyddsförordningen har organisationen tagit hjälp av den vägledning som SKL (Sveriges Kommuner och Landsting) tillhandahåller. Organisationen tycker inte att arbetet med formulering av samtyckestexter borde vara speciellt svårt. Dock har det visat sig vara en aning problematiskt.

#### **4.2.2 Behandling av personuppgifter**

För att följa dataskyddsförordningens regler finns det olika rättsliga grunder att stödja sig emot beroende av vilket IT-system som ska behandla personuppgifter.

*”Om man tar exempelvis journalsystemet så följer ju det redan patientdatalagen och patientdatalagen har väldigt stora krav redan, så följer man patientdatalagen då är det oftast redan förenligt med dataskyddsförordningen och då krävs det ingen justering”.*



Organisationen har en del ”hemmasnickrade IT-system” som inte följer dataskyddsförordningen eller patientdatalagen. Dessa IT-system kommer att behöva avvecklas eller förbättras med tvåfaktorsautentisering när dessa ska hantera patientuppgifter. Det finns också många IT-system som inte har någon bra loggningsfunktion vilket är ett krav enligt patientdatalagen. Organisationen arbetar nu med en informationssäkerhetsanalys i alla IT-system för att se hur personuppgifterna behandlas. Med hjälp av analysen tas en matris fram som i sin tur ska användas för att visa en skala över informationsmängder.

*”Det finns en standard som heter ISO-27 000 som är ett ledningssystem för informationssäkerhet som då listar vilka informationssäkerhetskrav man har”.*

Utifrån analysen (matrisen) kan sedan organisationen se vilka krav som ställs på IT-system och vilka åtgärder som måste genomföras. Detta görs för att dataskyddsförordningen ställer högre krav på säkerhetsåtgärder. Analysen kommer att användas som ett verktyg för att säkerställa att organisationen följer dataskyddsförordningen. Organisationen samlar nu in personuppgifter som är ”bra att ha” (slentrianmässigt insamlade):

*”När man inte riktigt vet vad man ska ha det till men om 5 år kanske jag vill ha det här. Då är ett exempel när man sparar Cv:n, när man annonserat en tjänst för så tänker ofta dom som ansvar för tillsättningen”.*

Organisationen tittar på olika sätt att göra personuppgifterna anonyma.

*”Att göra uppgifterna anonyma, då försvinner många krav i dataskyddsförordningen som finns. För då är det inte längre personuppgifter eftersom dessa inte går att härleda till en levande fysisk person”.*

Organisationen menar att anonymisering kan vara bra om personuppgifter behövs i forskningsändamål.

Något som organisationen jobbar med är rätten till utdrag ur register vilket anses vara svårt att lösa. *”Svårt att sköta det när det gäller personuppgiftsbehandling i löpande text, i e-post osv”.* Det arbetas med att ta fram nya rutiner för e-posthanteringen, gallringsrutiner samt att personalen ska radera e-post efter en viss tid. *”Vi måste ha ett bra stödsystem för att kunna göra dom här registerutdragen. För att kunna hitta alla behandlingar”.*

*”Det finns inget som vi känner att det här kommer vi aldrig klara. Det viktigaste är att vi har rutiner och dokumentation för hur vi ska lösa dom kvarstående frågetecken med dataskyddsförordningen”.*

Organisationen menar att ingen vet hur tillsyn från Datainspektionen kommer att gå till och vad de kommer att titta på. Detta gör att organisationen är beredd att vidta fler åtgärder om det skulle behövas för att följa dataskyddsförordningens regler.

### 4.3 Kommunen

Organisationen är en svensk kommun med cirka 6 500 anställda. Organisationen har ett IT-system för personaladministrering i form av en molntjänst. Det finns även många olika verksamhetssystem som behandlar medborgarnas personuppgifter. Det kan då handla om exempelvis elever i skolan, äldreboenden eller bygglovssökande. *”Vi har otroligt mycket personuppgifter i olika typer av system”.*

Organisationen anser att införandet av dataskyddsförordningen har varit positivt. *”Vi har fått upp ögonen på verksamheterna, att de behöver ha bättre kontroll över vilka personuppgifter de behandlar”*.

Tidigare problem har rört sig om vem som ska ta ansvar för behandlingen. *”Vem tar ansvar för att registrera in de olika behandlingar vi håller på med och liknande, så det har nog upplevts som lite jobbigt”*.

För att skapa en större medvetenhet om dataskyddsförordningen har organisationen valt att använda sig av webbutbildningar. Alla medarbetare (6 500 stycken) har under en tio veckors period haft korta lektioner (3 minuter) en gång i veckan rörande dataskyddsförordningen. Organisationen anser sig inte vara i mål med dataskyddsförordningen.

*”Vi har nog kommit ganska långt på vägen i alla fall. Vi har ökat medvetenheten i verksamheten ganska mycket och det skulle jag säga är tack vare dom här utbildningarna vi haft”*.

#### **4.3.1 Samtycke och samtyckestexter**

Tidigare har inte samtycketexterna levt upp till personuppgiftslagen vilket organisationen är medveten om.

*”Många gånger när man har använt samtycke så har man kanske bara haft en kort mening om att ”du samtycker till personuppgiftsbehandling i enlighet med personuppgiftslagen” och sen så har det inte varit något mer än så. Jag har inte ännu stött på någon som har varit tillräcklig, som skulle vara tillräcklig när förordningen träder i kraft då”*.

Organisationen har många olika typer av behandlingar som inte bygger på samtycke. *”Men ibland har vi samtycken och dom formuleringarna måste ju ändras”*. Organisationen stödjer sig i vissa fall på annan rättslig grund. Ett exempel på detta är skollagen och socialtjänstlagen. *”Vi har väldigt mycket olika lagstiftningar som styr”*.

Organisationen menar att samtyckestexterna nu ska stämma överens med hur den faktiska behandlingen av personuppgifter ser ut. *”Det måste absolut stämma överens, jag menar formuleringen och den faktiska behandlingen, det ska inte vara några konstigheter”*.

Organisationens dataskyddsombud har tillsammans med stöd från SKL (Sveriges Kommuner och Landsting) tagit fram en punktlista som respektive delverksamhet ska kunna ta del av. Denna punktlista ska användas för att formulera unika samtyckestexter inom respektive verksamhetsområde.

*”Vi kan inte skriva en samtyckestext som ska gälla för allt, för då blir det obegripligt. Man måste sätta sig i varje enskild behandling om vad man ska göra och hur man ska formulera samtyckestexten”*.

#### **4.3.2 Behandling av personuppgifter**

Organisationen har gjort analyser utifrån den personuppgiftsbehandling som idag finns för att avgöra hur känslig den är. Det har förekommit känsliga personuppgifter i en av organisationens molntjänster. *”Då har man ju lagt på en sådan enkel sak som en*

*tvåfaktorsautentisering, och det fanns ju inte innan*". Tvåfaktorsautentisering är något som organisationen ser som ett minimikrav.

För att inte samla in personuppgifter i onödan har organisationen kontrollerat sina IT-systemen och gjort vissa korrigeringar.

*"Hur ser det här systemet ut, hur är det utformat i förhållande till den information vi behöver. I vissa fall har man ju upptäckt i system att här har vi 20 fält men det är egentligen bara 10 (fält) som hör till det här ändamålet"*.

*"Regeln eller principen är ju inte ny om uppgiftsminimering, den gäller ju redan i personuppgiftslagen. Men vi har haft dålig koll på det"*.

Det har även införts ett filter som läser av när personalen försöker skicka känsliga personuppgifter som exempelvis personnummer via e-post. Organisationens säger att personuppgiftsincidenterna har halverats efter den interna webbutbildningen. Om IT-systemet känner av att personuppgifter kommer ett skickas med e-post får personen ett meddelande; *"Är du säker på att du vill göra det här?"*. *"Så att du tänker till i alla fall innan du gör det"*. Det finns nu också möjlighet att skicka informationen krypterad. Organisationens arbetar med att ta fram olika IT-lösningar för att kunna följa dataskyddsförordningen. *"Det kommer smågrejer hela tiden"*.

*"E-posten kommer att börja automat gallras den 25:de maj (2018). E-posten har blivit något i våra verksamheter som den inte har tänkt att vara. För den har blivit ett arkiv... Allt som är äldre än 6 månader gallras, i alla korgar. Och sen tror jag att borttagna korgen gallras allt som är äldre än en månad... Det som ska bevaras ska inte ligga i en enskild tjänstemans inkorg, utan det ska ligga i ett verksamhetssystem eller i ett diarieföringssystem"*.

Organisationen har infört ett nytt IT-system som ska känna igen om personuppgifter lagras någonstans i interna lagringsytor (hos anställda).

#### 4.4 Bostadsbolaget

Organisationen är ett svenskt bostadsbolag som äger cirka 6 000 bostäder. Organisationens har ungefär 40–50 olika IT-system. Många av systemen som används är fastighetsrelaterade och kundrelaterade. Det finns även IT-system som behandlar personalens personuppgifter. Fastighetssystemen är de IT-system som är de mest kritiska gällande dataskyddsförordningen. Organisationens personaladministrativa IT-system innehåller också känsliga personuppgifter och behöver därför ses över. Organisationens gör en risk- och säkerhetsanalys på samtliga IT-system.

Organisationen menar att de tog införandet av dataskyddsförordningen på stort allvar och tillsatte *"ganska stora resurser, vi är några stycken som jobbar med det"*. Organisationens har haft hjälp av extern expertis i form av en jurist.

*"Det är spännande, men det är tur att det inte är böter utan det är viten, då räknar man med att man blir tillsagt först. Och då får man försöka rätta till det i så fall. Vi försöker jobba mot GDPR för att stödja det ordentligt sen får vi väl höra om nån tycker något annat och då får vi ta hand om det då"*.

#### 4.4.1 Samtycke och samtyckestexter

Det finns en del skillnader som måste justeras i samtyckestexterna för att dessa ska följa dataskyddsförordningen. Organisationen har arbetat mycket med personuppgiftslagen tidigare och menar att det inte är speciellt stor skillnad.

*”Men utmaningar nej, vi har ganska bra koll på, vi har nog inte tagit så mycket onödigt, vi har nog följt det ganska bra. Vi har väl inte haft några större utmaningar när det kommer till samtyckestexter”.*

I dag hänvisar organisationen till personuppgiftslagen på sin webbplats i dess samtyckestexter. Nya samtyckestexterna planeras att publiceras samtidigt som dataskyddsförordningen träder i kraft.

Då organisationen behandlar personuppgifter om sina kunder krävs samtycke enligt en samtyckestext då ingen annan rättslig grund för behandlingen finns. *”Vi måste ha ett samtycke för att den registrerade ska veta vad vi ska använda uppgifterna till”.*

Organisationen har haft svårigheten att formulera sina samtyckestexter både informativt och lättbegripligt. *”Man ska informera om allt men det ska vara grundläggande och det är ju svårt”.*

*”Tillgänglighetsanpassningar på webben ska vara okej. Det finns andra språk som skulle vara viktigt men vi har inte översatt det till alla språk, vi har använt Google Translate där i dagsläget. Enligt våra hyresgäster tycker dom att det är bäst för om vi försöker översätta blir det oftast mer fel... Med Google Translate vet dom att det kan vara lite fel och då förstår dom innebörden av det, så har vi resonerat”.*

Organisationen tror att samtyckestexterna är tillräckligt informativa men är aningen osäkra. *”Det kan du inte fråga oss om, det måste du fråga hyresgäster om tror jag”.*

*”Det är så eftertraktat med bostäder idag så att dom skiter i vad det står, dom vill bara ha en bostad. För dom kommer inte vidare till sida två om dom inte godkänner. Jag vet inte, hur många tror ni läser det där?”.*

#### 4.4.2 Behandling av personuppgifter

Många av organisationens IT-systemen är standardsystem. *”Så det är ju att sätta press på leverantörerna att de stöttar oss i den här omställningen. Så att vi kan följa dataskyddsförordningen”.* Det som organisationen tittat extra på är att personuppgifterna sparas ändamålsenligt samt rätten att bli glömd. Organisationen har inget IT-system eller annat system för hur rätten att bli glömd ska hanteras utan blir en manuell fråga när det uppstår.

Organisationen har inte gjort några stora förändringar i sina IT-system utan endast beaktat hantering för avidentifiering. Organisationen ska inte behandla några personuppgifter i onödan.

*”IT-stödet förändras inte för att hjälpa oss upprätthålla den lagen eller vad man nu kallar det. Men vi har en rutin för hur vi ska göra och det är väl det viktigaste”.*

Avidentifiering är den största åtgärden som vidtagits för att följa dataskyddsförordningen. Det finns nu på förslag att gallring ska ske efter ospecificerat antal dagar. Denna gallring görs för att inte spara på personuppgifter i löpandet text under en längre tid (e-post). *”Vi*

*har en del ärenden som vi inte har någon bra rutin för att lyfta över till något system för ärendehantering än så länge". Hanteringen av personuppgifter i e-postmeddelanden menar organisationen kommer bli omöjligt att uppfylla.*

*"Gallring, det har vi inte haft förut. När man ska gallra dokument, det har vi gjort till stor del. Har ni bott hos oss för 10 år sedan så finns ingenting kvar. Inga obetalda hyror eller någonting. Då syns man inte i systemet, "systemen". Annars hade ni varit kvar om ni bott hos oss för 10 år sedan".*

*"Det pågår ett rejält rensningsarbete måste vi säga för bland annat bilder som har tagits på människor, dokument som folk har sparat över allt i hemkataloger och gemensamma fil-tytor. Vi har scannat igenom efter dokument som kan innehålla personuppgifter och det kan vara 1000-tals dokument".*

## 4.5 Banken

Organisationen är en svensk bank som tillhandahåller elektroniska betalningslösningar. Organisationen har många komplexa IT-system som är en kombination av egenutvecklade plattformar och externa e-tjänster. IT-systemen har byggts om flera gånger och är uppdelade i ett europeiskt och ett amerikanskt IT-system.

Organisationen började tidigt att arbeta med dataskyddsfrågor då det även tillsattes fem jurister för att lösa problematiken. Ledningen förstod tidigt att personlig integritet skulle komma att bli en viktig fråga i framtiden därav gjordes en stor satsning redan 2012.

*"Som tur är fokuserades det väldigt tydligt på det här sen 2012. Förhållandevis bra fokus på dataskyddet redan då. Men gjort ett antal förändringar ändå".*

Inställningen till dataskyddsförordningen har varit väldigt positiv inom organisationen. *"Inställningen är väldigt positiv och skälet till det är redan när jag började arbeta här 2012 hade man tydligt identifierat detta för att kunna bedriva verksamheten".*

### 4.5.1 Samtycke och samtyckestexter

Organisationen försöker att behandla alla personuppgifter utan att samla in samtycke.

*"Vi har en tydlig policy i att aldrig försöka använda samtycken. Det kanske inte har satt sig i branschen, men nu med GDPR är det fler och fler som förstår problematiken med att man inte ska samla in samtycken om man inte behöver".*

Organisationen menar att personuppgiftslagen följts under alla år och att införandet av dataskyddsförordningen inte kommer att ställa till med några större problem. Organisationen menar även att personuppgiftslagen lurat många att inhämta samtycke trots att annan rättslig grund finns.

*"Enligt Pul ser det ut som att samtycke är den väg man bord gå. Genom att behandla samtycke är det den främsta grunden för hur man gå få rätten att behandla personuppgifter".*

*"Samtycke har slängts in många gånger för att man är van med det. Den approachen har jag försökt att gå bort i från. Med GDPR har det här blivit tydligare".*

Organisationen arbetar mycket med att få avtal och texter att bli tillräckligt informativa för att användaren ska ges största möjlighet att förstå vad behandlingen innefattar.

*”Det ska finnas information till användaren med länkar till en personuppgiftspolicy med information om hur personuppgifterna behandlas. Men om vi ovanpå det lägger att den tillämpliga grunden för behandlingen ska vara samtycke då måste jag också i checkouts lägga till text på skärmen som verkligen tydliggör för dig som användare att: genom att gå vidare här så behöver du samtycka till behandlingen av personuppgifter i syfte att bla bla och så vidare”.*

#### **4.5.2 Behandling av personuppgifter**

Organisationen gör en del förändringar i sina IT-system för att kunna följa dataskyddsförordningens regler. Något som har visat sig vara extra utmanande är lagringsminimering och gallring.

*”Vad som särskilt är utmanande här det är sånt som gallring, dom registrerades rättigheter... Det har tillkommit ett antal nya rättigheter med möjlighet att frysa behandling. Det är sånt som inte har funnits i plattformarna idag”.*

Det har även arbetats med att få behandlingen att stämma överens med vad texterna säger. *”Vi har arbetat med att kartlägga att behandlingen stämmer överens med vad som står”.*

Vad organisationen nu arbetar med är att ta fram en lösning för hur IT-systemen på bästa sätt ska visa den information som texterna innefattas av. Vilken ordning och hur mycket information som ska presenteras i olika skärmbilder med mera. Detta för att få den registrerade att läsa all informationen och på så sätt skapa förtroende.

*”Men det ofta det som genererar ett annat problem och det är om man har för mycket information så orkar inte folk läsa. Man måste bygga det på något sätt, kanske i olika steg”.*

## 5 Analys

I det här kapitlet presenteras studiens analys. Utifrån genomförda intervjuer kommer det empiriska materialet att ställas mot dokument- och litteraturstudier. Underrubrikerna ska hjälpa läsaren att på ett enklare sätt förstå analysens upplägg vilket motsvarar två teman. Studiens empiriska data kommer att sammanfattas i två tabeller. Sammanfattade tabeller kommer att belysa utmaningar och åtgärder rörande samtyckestexter och behandlingen av personuppgifter. Tabellerna kommer även att förtydligas och analyseras i löpande text. I slutet av respektive tema analyseras organisationerna emot varandra.

### 5.1 Organisationernas samtyckestexter enligt dataskyddsförordningen

I Tabell 5 visas en sammanfattning av respektive organisations utmaningar och åtgärder gällande samtyckestexter. Förklaring av tabellen ges under rubrikerna för respektive organisation.

	Landstinget	Kommunen	Bostadsbolaget	Banken
Utmaningar	<ul style="list-style-type: none"><li>- Låg kunskap</li><li>- Informativt (transparent)</li><li>- Återkalla samtycke</li><li>- Färdigställa samtyckestexter</li></ul>	<ul style="list-style-type: none"><li>- Låg kunskap</li><li>- Informativt (transparent)</li><li>- Inte följt PuL tidigare</li><li>- Färdigställa samtyckestexter</li></ul>	<ul style="list-style-type: none"><li>- Låg kunskap (transparent)</li><li>- Osäkerhet</li></ul>	<ul style="list-style-type: none"><li>- Informativt (transparens)</li></ul>
Åtgärder	<ul style="list-style-type: none"><li>- Undvika samtycke</li><li>- Process för att återkalla samtycke</li><li>- Dokumenterat samtycke</li><li>- Formulera informativa samtyckestexter</li></ul>	<ul style="list-style-type: none"><li>- Undvika samtycke</li><li>- Formulera informativa samtyckestexter</li><li>- Formulera unika samtyckestexter</li></ul>	<ul style="list-style-type: none"><li>- Extern expertis</li><li>- Inhämta samtycke för att skapa rättslig grund</li><li>- Formulera informativa samtyckestexter</li></ul>	<ul style="list-style-type: none"><li>- Undvika samtycke</li></ul>

Tabell 5: Organisationernas utmaningar och åtgärder gällande samtyckestexter.

#### 5.1.1 Landstinget

Utmaningar med samtyckestexter som organisationen ställs inför innefattar; låg kunskap, formulera informativa samtyckestexter, återkalla samtycke samt färdigställa sina samtyckestexter (Tabell 5). Med låg kunskap menas att många i organisationen inte tror att personuppgifter får behandlas överhuvudtaget. Organisationen behöver även införa en process för att den registrerade ska kunna återkalla sitt samtycke vid behandlingen av dennes personuppgifter. Organisationen behöver även färdigställa sina samtyckestexter.

Åtgärder som vidtagits för att möta dataskyddsförordningen är först och främst att försöka undvika samtycken. Då organisationen kan ställa sig emot andra rättsliga grunder som exempelvis patientdatalagen är det ett bra val av organisationen att inte inhämta samtycke i onödan. Enligt Datainspektionen (2017) finns det flera rättsliga grunder som organisationen kan luta sig emot. Rättslig förpliktelse innebär att det krävs av annan lag att personuppgifter behandlas. Personuppgifter får även behandlas av grundläggande intresse, exempel på detta är om den registrerade är medvetlös och inte kan lämna sitt samtycke vid behandlingen (ibid.). Det är viktigt att kunna visa vilken rättslig grund som organisationen valt att luta sig emot menar Bhaimia (2018). Detta är något som organisationen är medveten om.

Organisationen har ännu ingen process för hur samtycke ska kunna återkallas av den registrerade vilket är ett problem då detta krävs för ”giltigt samtycke” (European Parliament, 2017). Organisationen har tankar om en funktionsbrevlåda eller en avdelning som den registrerade ska kunna vända sig till för att återkalla samtycke. Detta motstrider vad dataskyddsförordningen säger såvida inte samtycke också lämnats på samma sätt (ibid.).

Organisationen har valt att samla in samtycke i skriftlig form vilket är ett av alternativen i skäl 32 (Europaparlamentets och rådets förordning (EU) 2016/679).

För att ta fram informativa samtyckestexter är organisationen medveten om att dessa inte ska vara långa juridiska texter. Noain-Sánchez (2016) menar att det bör finnas tillräcklig med information om hur personuppgifterna kommer att behandlas och att den registrerade ska förstå behandlingens syfte (ibid.). Samtyckestexterna är ännu inte helt klara men organisationen tar hjälp av SKL (Sveriges Kommuner och Landsting) för att färdigställa dessa.

### 5.1.2 Kommunen

Utmaningar med samtyckestexter som organisationen ställs inför innefattar; låg kunskap, formulera informativa samtyckestexter, inte tidigare följt personuppgiftslagen samt färdigställa sina samtyckestexter (Tabell 5). Med låg kunskap menas att många i personalen inte vet vad dataskyddsförordningen innefattar. Organisationen har inte tidigare följt personuppgiftslagen vilket gör att anpassningen till dataskyddsförordningen blir svårare att genomföra.

Åtgärder som vidtagits för att följa dataskyddsförordningen är att undvika inhämtning av samtycke. Att undvika samtycke kan ses som ett smart upplägg då samtycken är en sista utvägen för att skapa rättslig grund (Datainspektionen, 2017). Dock kommer organisationen att behöva inhämta samtycken i specifika fall.

Bhaimia (2018) beskriver att samtyckestexterna måste vara informativa till den registrerade. Då organisationen måste skriva separata samtycketexter för respektive verksamhetsområde gäller det att samtliga texter utformas tillräckligt informativt. Att skriva informativa samtyckestexter kan bli en utmaning då organisationen inte tidigare följt personuppgiftslagen. Att åtgärda tidigare samtyckestexter (enligt PuL) kommer att bli ett stort steg då organisationens samtyckestexter aldrig varit tillräckliga informativa.

*”Jag har inte ännu stött på någon som har varit tillräcklig, som skulle vara tillräcklig när förordningen träder i kraft då”.*

Jørgensen och Desai (2017) förklarar att brister som tidigare funnits i samtycken förbättras med hjälp av dataskyddsförordningens nya regler eftersom kraven ökat. Detta kan ses som positivt då organisationen är införstådd med vad dataskyddsförordningen säger om personuppgiftsbehandlingen.

Samtyckestexterna är ännu inte klara då det är upp till varje enskild delverksamhet att formulera sina egna texter för respektive ändamål. För att skapa större kunskap i organisationen har alla medarbetare genomfört webbutbildningar om dataskyddsförordningen. Utbildningarna har visat på positiva effekter då personuppgiftsincidenterna minskat.



### 5.1.3 Bostadsbolaget

Utmaningar med samtyckestexter som organisationen ställs inför innefattar; låg kunskap, osäkerhet och att kunna formulera informativa samtyckestexter (Tabell 5).

Organisationen har tillsatt resurser som ska arbeta med dataskyddsfrågor. Utöver intern expertis har organisationen tagit in extern expertis i form av en jurist. Organisationen har varit tvungen att formulera nya samtyckestexter för att kunna inhämta samtycken. *”Vi måste ha ett samtycke för att den registrerade ska veta vad vi ska använda uppgifterna till”*. Organisationen är med detta medveten om att rättslig grund krävs för behandlingen av personuppgifter. Datainspektionen (2017) ser dock samtycke som en sista utväg för att få behandla personuppgifter.

Organisationen är medveten om att samtyckestexterna ska vara informativa och lättbegripliga. Appelgren (2017) menar att den registrerades medvetenhet om behandlingen ska öka vid införandet av dataskyddsförordningen. Organisationen tycker att formuleringen av samtyckestexter varit svårt. *”Man ska informera om allt men det ska vara grundläggande och det är ju svårt”*.

Ytterligare åtgärder som organisationen vidtagit för att skapa informativa samtyckestexter är att översätta texterna med hjälp av Google Translate. *”Med Google Translate vet dom att det kan vara lite fel och då förstår dom innebörden av det, så har vi resonerat”*. Att informationen kan vara felaktig går emot vad informativt samtycke innebär (Noain-Sánchez, 2016). Noain-Sánchez (ibid.) menar att informationen måste framgå tydligt för att den registrerade ska känna sig självständig.

Organisationen menar att den registrerade inte bryr sig om vad det står i samtyckestexterna. Detta uttryck kan tolkas som att organisationen inte tar reglerna angående informativt samtycke på allvar med beaktning av följande citat:

*”Det är så eftertraktat med bostäder idag så att dom skiter i vad det står, dom vill bara ha en bostad. För dom kommer inte vidare till sida två om dom inte godkänner. Jag vet inte, hur många tror ni läser det där?”*

Detta visar att organisationen tror sig kunna formulera samtyckestexterna hur som helst för att den registrerade i detta fall är i beroendeställning. Noain-Sánchez (2016) menar att den registrerade ska ha kännedom om behandlingen och få en känsla av att god integritet upprätthålls.

### 5.1.4 Banken

Utmaningar med samtyckestexter som organisationen ställs inför innefattar att göra dessa informativa (Tabell 5). För att skapa informativa avtal och texter har organisationen anlitat flera jurister.

*”Det ska finnas information till användaren med länkar till en personuppgiftspolicy med information om hur personuppgifterna behandlas. Men om vi ovanpå det lägger att den tillämpliga grunden för behandlingen ska vara samtycke då måste jag också i checkouts lägga till text på skärmen som verkligen tydliggör för dig som användare att: genom att gå vidare här så behöver du samtycka till behandlingen av personuppgifter i syfte att bla bla och så vidare”*.

Detta visar att organisationen vill att den registrerade ska förstå på ett tydligt sätt vad informationen säger. Noain-Sánchez (2016) menar att det bör finnas tillräckligt med information för att den registrerade ska förstå syftet med behandlingen. Organisationen

arbetar med att skapa bättre flöden för hur samtyckestexterna ska presenteras på den registrerades skärmbild.

Åtgärder som vidtagits sedan flera år tillbaka är att organisationen försöker att stödja sig på annan rättslig grund än samtycke. Detta kan ses som positivt då sista utvägen för att få behandla personuppgifter är att inhämta samtycke om ingen annan rättslig grund finns (Datainspektionen, 2017). Organisationen menar att samtycke inte ska inhämtas i onödan då det kan skapa problematik.

### **5.1.5 Skillnader och likheter mellan organisationerna**

Tre av fyra organisationer har låg kunskap internt gällande dataskyddsförordningen. Mest pålästa är Banken (privat sektor) som har arbetat med dataskyddsfrågor under en längre tid. Det finns alltså inga mönster kunskapsmässigt gällande privat och offentlig sektor i detta avseende. Utmaningar som kan ses hos samtliga organisationer är att kunna formulera informativa samtyckestexter. Att färdigställa samtyckestexterna har visat sig vara ett större problem inom den offentliga sektorn. Inom den privata sektorn är organisationerna klara med sina samtyckestexter och har satt upp ett datum för publicering. Vad som tidigare har analyserats är att Bostadsbolaget och Banken har olika syn på samtyckestexter. Bostadsbolaget engagerar sig mindre i utformandet av samtyckestexterna medan Banken vill skapa ett stort förtroende till den registrerade genom god information. Detta visar två olika attityder till samtyckestexter inom den privata sektorn. Tre av fyra organisationer försöker att inte använda sig av samtycke utan istället finna annan rättslig grund för behandlingen. Bostadsbolaget är dock väldigt tydliga med att samtycke krävs för att kunna bedriva sin verksamhet. Organisationerna visar med detta att det finns en större förståelse för hur samtycke bör användas. Detta är något som förändrats i samband med dataskyddsförordningen. Även Jørgensen och Desai (2017) menar att brister som tidigare funnits i samtyckestexterna förbättras med hjälp av dataskyddsförordningen.

## **5.2 Organisationernas behandling av personuppgifter enligt dataskyddsförordningen**

*I Tabell 6 presenteras en sammanfattning av respektive organisations utmaningar och åtgärder gällande behandlingen av personuppgifter. Förklaringar av tabellen ges under rubrikerna för respektive organisation.*

	Landstinget	Kommunen	Bostadsbolaget	Banken
<b>Utmaningar</b>	<ul style="list-style-type: none"> <li>- IT-system med felaktiga personuppgifter</li> <li>- Loggningsfunktion</li> <li>- Uppgiftsminimering</li> <li>- IT-verktyg för registerutdrag</li> </ul>	<ul style="list-style-type: none"> <li>- Ansvar för behandling</li> <li>- Inte följt PuL tidigare</li> <li>- Rutiner för gallring</li> </ul>	<ul style="list-style-type: none"> <li>- IT-system med felaktiga personuppgifter</li> <li>- Rätten att bli glömd</li> <li>- IT-verktyg för ärendehantering</li> <li>- Ostrukturerade personuppgifter (e-post)</li> </ul>	<ul style="list-style-type: none"> <li>- Komplexa IT-system</li> <li>- Gallring</li> <li>- Uppgiftsminimering</li> </ul>
<b>Åtgärder</b>	<ul style="list-style-type: none"> <li>- Tvåfaktorsautentisering</li> <li>- Kategorisering</li> <li>- Säkerhetskrav</li> <li>- Avidentifiering</li> <li>- Gallring</li> <li>- Riskhanteringsplan</li> </ul>	<ul style="list-style-type: none"> <li>-</li> <li>- Tvåfaktorsautentisering</li> <li>- Webbutbildning</li> <li>- Analys av behandlingen</li> <li>- IT-verktyg</li> <li>- Gallring</li> </ul>	<ul style="list-style-type: none"> <li>- Riskanalys av IT-system</li> <li>- Uppgiftsminimering</li> <li>- Rutiner för incidenter</li> <li>- Gallring</li> </ul>	<ul style="list-style-type: none"> <li>- Förändringar av IT-system</li> </ul>

Tabell 6: Organisationernas utmaningar och åtgärder gällande behandlingen av personuppgifter.

### 5.2.1 Landstinget

Organisationen står inför ett antal utmaningar när det kommer till behandling av personuppgifter i enlighet med dataskyddsförordningen. Dessa utmaningar är IT-system med felaktiga personuppgifter, loggningsfunktion och uppgiftsminimering men även IT-verktyg för registerutdrag (Tabell 6). En utmaning för organisationen är att identifiera IT-system som innehåller felaktiga personuppgifter. IT-systemens förmåga att säkerställa ett dataskydd som är i enlighet med dataskyddsförordningen varierar (Datainspektionen, 2017).

Det har varit en utmaning för organisationen att säkerställa en fungerande loggningsfunktion som ska vara i enlighet med patientdatalagen. Loggningsfunktionen används för att avslöja säkerhetsavvikelser som till exempel olovlig åtkomst (Datainspektionen, 2017). En säker loggningsfunktion är inte en regel som finns i dataskyddsförordningen. Loggningsfunktionen bör säkerställas för att få behandla personuppgifter utifrån rättslig grund enligt patientdatalagen. Loggningsfunktionen kan inte garanteras vilket innebär att det inte finns något stöd enligt rättslig grund för behandling av personuppgifter. Detta innebär att organisationen inte kan stödja sig mot någon rättslig grund vid behandling av personuppgifter enligt dataskyddsförordningen.

Organisationen samlar in personuppgifter slentrianmässigt för behandling utan ett ändamålsenligt syfte. Detta uppfyller inte kravet på ändamålsenlighet som är ett tillägg i dataskyddsförordning (Datainspektionen, 2017).

Det är en utmaning för organisationen att finna ett IT-verktyg som kan söka information om alla personuppgiftsbehandlingar. Detta IT-system ska kunna göra registerutdrag till den registrerade där all information som rör dennes behandling ska visas. Den registrerade har rätt enligt dataskyddsförordningen att få ett registerutdrag på hur dennes personuppgifter behandlas (Datainspektionen, 2017).

Organisationen har vidtagit åtgärder med hänsyn till att säkerställa lämplig åtkomst av IT-system. Organisationen har planer på att införa tvåfaktorsautentisering som ett ytterligare skydd mot felaktig åtkomst av IT-system. Enligt dataskyddsförordningen bör organisationer vidta lämpliga åtgärder för att undvika dataintrång då ett intrång kan innebära negativa konsekvenser för den registrerade (Datainspektionen, 2017). I skäl 84 (Europaparlamentets och rådets förordning (EU) 2016/679) står det att

personuppgiftsansvarige ska vara ansvarig för att en konsekvensbedömning utförs avseende dataskydd, framförallt genom att bedöma riskens ursprung, art, särdrag och allvar.

Organisationen genomför en informationssäkerhetsanalys som är en åtgärd till att säkerställa hur personuppgifter behandlas. IT-systemen analyseras för att få en bild av vilka personuppgifter IT-systemen innehåller. För att illustrera personuppgifter har en matris skapats. Matrisen tillhandahåller en skala där det ska framgå i vilken grad personuppgifterna är kritiska. Organisationen har använt sig av ett standardiseringsverktyg (ISO 27000). Det verktyget är framtaget för att organisationer ska kunna säkerställa en förstärkt kontroll av sina IT-system och personuppgifter.

Att upprätta ett personuppgiftsbehandlingsregister kan anses vara en åtgärd som är i linje med kommande dataskyddsförordning. Datainspektionen (2017) kan vid en tillsyn begära att få se personuppgiftsbehandlingsregistret. Åtgärden att upprätta ett register bör vidtas för att leva upp till dataskyddsförordningen.

Organisationen har även påbörjat arbetet med att ta fram rutiner för e-posthantering och gallring. Detta i syfte att inte lagra och behandla personuppgifter som inte uppfyller kravet för ändamålsenlighet i dataskyddsförordningen.

## 5.2.2 Kommunen

Organisationen har medgett att det finns utmaningar inför omställningen till dataskyddsförordningen. En utmaning är att se över sina IT-system för att kunna ta ansvar för behandlingen av personuppgifter. Det som har varit en utmaning för organisationen är att utse vem det är som ska ansvara för att registrera behandlingarna. Det har även visat sig vara en utmaning för organisationen att samla in och behandla personuppgifter för att uppfylla kravet på ändamålsbegränsning (Artikel 5, Europaparlamentets och rådets förordning (EU) 2016/679). Organisationen medger att regler vidkommande uppgiftsminimering i enlighet med personuppgiftslagen inte har fullgjorts. En utmaning som organisationen står inför är att leva upp till regeln om uppgiftsminimering som är ett tillägg i dataskyddsförordningen (Datainspektionen, 2017).

Det har även visats sig vara en utmaning att gallra personuppgifter som finns i organisationens IT-system. Det har visats sig vara svårt att följa nuvarande lagstiftning med hänsyn till gallring enligt personuppgiftslagen.

*”E-posten kommer att börja automat gallras den 25:de maj (2018). E-posten har blivit något i våra verksamheter som den inte har tänkt att vara. För den har blivit ett arkiv”*

Organisationen har analyserat nuvarande personuppgiftsbehandling för att få kontroll över personuppgifter som finns inom verksamhetens IT-system. Informationssäkerhetsanalys har genomförts för att få insikt i hur känslig rådande behandling är utifrån de regler som finns i dataskyddsförordningen. Organisationen har även vidtagit förebyggande åtgärder som tvåfaktorsautentisering.

I avsikt att undvika tillbud som i dataskyddsförordningen tillskrivs som personuppgiftsincidenter är organisationen skyldiga att vidta åtgärder som kan förstärka dataskyddet (Datainspektionen, 2017). Organisationen använder ett IT-verktyg som kan upptäcka och identifiera personuppgifter i e-post. IT-verktyget varnar den anställde om någon personuppgift försöker skickas med e-post.

Organisationen har vidtagit en åtgärd för att identifiera personuppgifter som kan finnas lagrade hos den anställdas digitala utrymmen. Denna åtgärd har utformats för att de

anställda inte ska förvara personuppgifter som saknar ändamålsenlighet (Datainspektionen, 2017).

### 5.2.3 Bostadsbolaget

Organisationen uppgav att det finns ett flertal IT-system som hanterar personuppgifter i dagsläget. IT-systemen som finns inom organisationen är standardsystem. Organisationen uppger att det finns en utmaning i att få leverantörerna av IT-systemen att modifiera systemen så att de behandlar personuppgifter i enlighet med dataskyddsförordningen.

Organisationen uppger att de inte har något IT-verktyg eller någon automatiserad process för rätten att bli glömd. I dagsläget hanteras ärenden med hänsyn till rätten att bli glömd manuellt. Organisationen ser utmaningar i den manuella hanteringen. Dessa utmaningar kan innebära svårigheter för organisationen att uppfylla de registrerades rättighet om att få sina personuppgifter raderade. Den registrerade har enligt dataskyddsförordningen rätt att via dokument eller i annan form få ta del av de personuppgifter som kan vara lagrade i organisationens IT-system (Datainspektionen, 2017). Organisationen uppger att de i dagsläget inte har någon möjlighet att hantera dessa ärenden då rutiner för ärendehantering saknas men även lämpligt systemstöd.

Organisationen ser utmaningar i den nuvarande personuppgiftshanteringen avseende e-post. Organisationen menar att det kommer att vara svårt att uppfylla de regler som avser personuppgiftshanteringen då det finns en problematik i den nuvarande behandlingen av ostrukturerade personuppgifter. I dataskyddsförordningen framgår det tydligt att det bör utföras en bedömning på den e-post som hanteras för att kunna avgöra ifall behandlingen utförs korrekt (Datainspektionen, 2017).

Organisationen har uppgett att de vidtagit åtgärder för att stärka sitt dataskydd. Åtgärderna som genomförts är riskanalyser och säkerhetsanalyser av IT-system. Organisationen uppger att de fokuserat på att personuppgifter ska lagras ändamålsenligt. Organisationens mål är att ändamålsenligt lagra och behandla personuppgifter, vilket är i linje med kommande dataskyddsförordning (Datainspektionen, 2017). Organisationen uppger att de har ambition att skapa en rutin för rätten att bli glömd samt för att personuppgifter ska behandlas ändamålsenligt (ibid.). Organisationen förklarade att det finns ett pågående arbete med att söka upp och identifiera uppgifter som finns i IT-systemen. Arbetet syftar till att gallra personuppgifter som saknar laglig grund för behandling.

### 5.2.4 Banken

Det har för organisationen inneburit en utmaning att anpassa IT-systemen så att de lever upp till dataskyddsförordningen och dess regler. Organisationen har vidtagit åtgärder gällande sina IT-system i syfte att förändra och anpassa de till dataskyddsförordningen. Organisationen har upplevt det som utmanande att säkerställa rätten att bli glömd. Praktiskt för organisationen innebär detta att söka, identifiera och slutligen gallra uppgifter som önskats av den registrerade.

Det har visat sig vara en utmaning för organisationen att gallra personuppgifter som är överflödiga. Detta då dataskyddsförordningen innefattar kravet på uppgiftsminimering (Datainspektionen, 2017). Regeln om uppgiftsminimering innebär praktiskt för organisationen att endast behandla och lagra uppgifter under en begränsad tid. De får enbart behandla personuppgifter om det finns rättslig grund (ibid.). Organisationen har även vidtagit åtgärder gällande sina IT-system i syfte att förändra och anpassa de till dataskyddsförordningen.

### **5.2.5 Skillnader och likheter mellan organisationerna**

Två av fyra organisationer har upplevt det som problematiskt att hantera de stora mängder personuppgifter som finns spridda över respektive organisations IT-system. Kommunen har uttryckt att det inte finns utmaningar i att hantera dessa mängder med personuppgifter. Kommunen har uppgett att det finns utmaningar i att följa personuppgiftsbehandlingen i enlighet med personuppgiftslagen. Banken har uppgivit att det finns utmaningar i hanteringen av personuppgifter baserat på de komplexa IT-system som finns inom organisationen. Det finns en tydlig utmaning i hanteringen av personuppgifter vilket är genomgående för alla organisationer. Det framgår även att det finns en genomgående utmaning i att uppfylla kravet om uppgiftsminimering och lagringsminimering inom samtliga organisationer. Alla organisationer ser utmaningar med att automatiskt hantera personuppgifter som finns spridda inom organisationernas IT-system. Landstinget, Kommunen och Bostadsbolaget har vidtagit mindre åtgärder för att följa dataskyddsförordningens regler. De tekniska åtgärderna som organisationerna har uppgett att de vidtagit är tvåfaktorsautentisering, aidentifiering samt införandet av IT-verktyg. De åtgärder som är av icke teknisk karaktär är informationssäkerhetsanalyser, rutiner och incidenthanteringsplaner. Det finns inga tydliga mönster mellan privat och offentlig sektor.

## 6 Diskussion

*I detta kapitel kommer vi att diskutera organisationernas utmaningar och åtgärder i relation till befintlig litteratur som tidigare presenterats. Kapitlet är uppdelat i två underrubriker för att tydligare särskilja forskningsfrågorna. Först diskuteras organisationernas samtyckestexter och avslutningsvis diskuteras organisationernas behandling av personuppgifter.*

### 6.1 Organisationernas samtyckestexter enligt dataskyddsförordningen

Låg kunskap är ett genomgående mönster som kan utläsas i tre av fyra organisationer. Det har visat sig att Landstinget, Kommunen och Bostadsbolaget besitter låga kunskaper där många anställda inte är medvetna om vad dataskyddsförordningen innefattar. Banken har däremot högre kunskap eftersom de sedan 2012 aktivt arbetat med dataskyddsfrågor. Kommunen har visat sig framgångsrika i denna fråga genom att försöka lösa problematiken med webbutbildningar vilket har upplevts som positivt inom organisationen. Att använda sig av webbutbildningar anser även vi vara positivt då utbildningen höjer deras befintliga kunskap. Kritik som kan riktas emot utbildningarna är dess minimala längd och omfattning. Problematiken med den låga kunskap som finns inom organisationerna är att jurister och dataskyddsombud blir högt belastade och måste hjälpa delverksamheterna med formuleringar av samtyckestexter. Detta trots att tydliga riktlinjer finns. Att anordna utbildning för att stärka kunskapen om dataskyddsförordningen är något alla organisationer bör eller redan borde ha tänkt på. Detta eftersom organisationerna vet med sig att det finns stora kunskapsbrister. Utbildningar skulle kunna ses som en åtgärd för framtiden innan nya lagar och förordningar träder i kraft. Vi kan inte utläsa att det finns något mönster mellan privat och offentlig sektor gällande ämnets kunskapsläge. Det som kan utläsas är att den organisation som arbetat med dataskyddsfrågor under längst tid också har mest kunskap inom området.

Rättslig grund för att behandla personuppgifter är något alla organisationer talar om, både inom privat och offentlig sektor. Tre av fyra organisationer vill helst inte använda samtycke utan målet är att stödja sig på annan rättslig grund. Inom den offentliga sektorn kan vi se att båda organisationerna försöker finna annan rättslig grund för behandlingen. Citat från Banken:

*”Samtycke har slängts in många gånger för att man är van med det. Den approachen har jag försökt att gå bort i från. Med GDPR har det här blivit tydligare”.*

Att organisationerna nu har förstått att samtycke är en sista utväg för behandlingen av personuppgifter anser vi vara positivt då även Datainspektionen (2017) menar att det är en sista utväg. Många gånger finns annan rättslig grund men organisationerna tar för vana att använda samtycke. Jørgensen och Desai (2017) menar att organisationer nu i allmänhet är mer påläsa om lagtext. Bostadsbolaget ser vi dock inte vara lika pålästa om dataskyddsförordningen och dess syfte då det gäller samtyckestexter. Citat från Bostadsbolaget: *”Vi måste ha ett samtycke för att den registrerade ska veta vad vi ska använda uppgifterna till”.* Det stämmer att organisationen måste inhämta ett samtycke från den registrerade för att få behandla en del av personuppgifterna. Det finns dock en anmärkningsvärd attityd till samtyckestexter vilket kan utläsas av följande citat:

*”Det är så eftertraktat med bostäder idag så att dom skiter i vad det står, dom vill bara ha en bostad. För dom kommer inte vidare till sida två om dom inte godkänner. Jag vet inte, hur många tror ni läser det där?”.*

Med detta uttalande kan vi utläsa att Bostadsbolaget (privat sektor) inte förstår i vilket syfte samtyckestexterna ska användas. Noain-Sánchez (2016) menar att den registrerade måste förstå syftet med behandlingen. Eftersom Bostadsbolaget använder samtycke som rättslig grund är det enligt oss förvånande att samtyckestexterna inte tas på större allvar vilket kan få konsekvenser i framtiden.

Med införandet av dataskyddsförordningen har det talats mycket om att behandlingen av personuppgifter ska vara transparent och med det menat att samtyckestexter och avtal ska vara informativa (Noain-Sánchez, 2016). Ett tydligt mönster som analyserats var att samtliga organisationer talade om problematiken i att formulera samtyckestexter som är tillräckligt informativa. Samtliga organisationer arbetade utifrån riktlinjer från externa jurister för att ta fram samtyckestexter. Utmärkande var att Banken fördjupat sig i frågan för att kunna tydliggöra sina avtal och samtyckestexter. Genom vältänkt interaktionsdesign vill Banken presentera informationen i ett sådant flöde som gör att den registrerade tar del av all information i avtalet och/eller i samtyckestexten. Genom detta anser vi att organisationens mål med samtyckestexter lever upp till syftet med dataskyddsförordningen. Som nämnts tidigare genom citaten visar inte Bostadsbolaget samma attityd till samtyckestexter. Det spelar således ingen roll att både Bostadsbolaget och Banken är av privat karaktär då båda dessa organisationer ser olika på frågan.

Övriga åtgärder varierar i stor grad och det finns mycket organisationerna skulle kunna lära sig av varandra. Det finns tyvärr inget mönster i vilken organisation eller i vilken sektor som förhållit sig bäst gällande samtyckestexter.

## 6.2 Organisationernas behandling av personuppgifter enligt dataskyddsförordningen

Organisationerna vi har intervjuat kan generellt inte anses leva upp till dataskyddsförordnings regler gällande sin personuppgiftsbehandling. Banken följer fler regler än de övriga organisationerna. Banken kan enligt oss i nuläget anses vara väl förberedd för omställningen. Utifrån analysen anser vi att de övriga organisationerna i dagsläget inte uppfyller dataskyddsförordningen. Det är för tidigt att säga ifall organisationerna kommer att ha uppfyllt de regler som dataskyddsförordningens innefattar eller inte. Detta eftersom lagen inte börjat gälla vid tidpunkten för studiens slutförande.

En utmaning som är gemensam inom organisationerna är mängden personuppgifter som finns inom IT-systemen. Personuppgifterna som är av strukturerad och ostrukturerad karaktär finns spridda över den digitala infrastrukturen. Dessa kvantiteter med uppgifter som finns inom organisationen har tillsammans med avsaknaden av relevanta IT-verktyg, kommit att stå för en mängd utmaningar. Tillräckliga förutsättningar att kunna behandla dessa kvantiteter med personuppgifter är grundläggande för att vara i enlighet med dataskyddsförordningen. De personuppgifter som finns spridda inom organisationerna innebär stora utmaningar för att uppnå krav om bland annat uppgiftsminimering, registerutdrag och gallring. Det behövs lämpliga tekniska åtgärder för att skydda informationen som finns om de registrerade. Organisationerna uppger gemensamt att det är svårt att lokalisera och identifiera uppgifter som kan hänföras till personuppgifter.

För att behandla personuppgifter i linje med kommande dataskyddsförordning bör organisationerna vidta tekniska åtgärder redan i utvecklingen av IT-system. Inbyggd integritet är ett tillägg i dataskyddsförordningen som tidigare inte har funnits i personuppgiftslagen. Tillägget har uppkommit då det finns krav på att IT-system ska anpassas med dataskydd under hela livscykeln. Principen inbyggd integritet kompletteras



av reglerna lagringsminimering och uppgiftsminimering. Organisationerna har i regel upplevt stora utmaningar i att vidta tekniska åtgärder för att uppfylla kraven om lagringsminimering och uppgiftsminimering.

En av organisationerna har skapat manuella register för att få kontroll över sina uppgifter. De har kategoriserat uppgifterna efter känslighet. Organisationen har också genomfört en informationssäkerhetsanalys i syfte att identifiera och kategorisera uppgifter för att få bättre kontroll. Det kan enligt oss anses vara en svår uppgift att manuellt föra ett register och kategorisera de uppgifter som finns inom ett komplext IT-system.

Det har framkommit att det inom en av organisationerna används ett IT-verktyg som är begränsat till e-post. IT-verktyget är effektivt i syfte att identifiera personuppgifter som kan förekomma i e-post. IT-verktyget varnar användaren om att känsliga uppgifter behandlas i e-post och användaren får sedan avgöra ifall denne vill exkludera personuppgifterna eller inte. Behovet av systemstöd för att identifiera och registrera personuppgifter är essentiellt i syfte att följa kravet om inbyggd integritet.

Det bör även nämnas att det inom de flesta organisationerna upprättats rutiner för behandlingen av personuppgifter och eventuella personuppgiftsincidenter. Detta är en åtgärd som är i linje med dataskyddsförordningen.

Det kan diskuteras i vilken grad varje vidtagen åtgärd stödjer sig mot respektive regel i dataskyddsförordningen. Det kan vidare diskuteras vilka och hur åtgärderna ska prioriteras. Det kan med säkerhet sägas att det krävs åtaganden som generellt sett inte kan anses vidtagna gällande behandling av personuppgifter inom organisationerna. Genom att ha den personliga integriteten i beaktning under IT-systemens livscykel, kan preventiva åtgärder vidtas för att undvika eller bemöta utmaningar som kan bli aktuella för att följa dataskyddsförordning.

## 7 Slutsatser

*I det här kapitlet presenteras studiens slutsatser genom att svara på frågeställningarna. Slutligen presenteras studiens kunskapsbidrag och förslag på vidare forskning.*

### 7.1 Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att utforma samtyckestexter i enlighet med dataskyddsförordningen?

Ett genomgående mönster hos samtliga organisationer är utmaningarna med att utforma informativa samtyckes- och avtalstexter i enlighet med dataskyddsförordningen. Alla studiens organisationer är medvetna om att dataskyddsförordningen ställer högre krav på att lämna tillräcklig information till den registrerade. Samtliga organisationer arbetar med att formulera texter som ska följa dataskyddsförordningens regler. Ifall behandlingen av personuppgifter inom en organisation inte uppfyller dataskyddsförordningens regler så har inte heller formuleringen av informativa samtyckestexter någon betydelse. Både behandling av personuppgifter och informativa samtyckestexter ska vara i enlighet med dataskyddsförordning då dessa områden kompletterar varandra.

Alla organisationer är medvetna om att det krävs en rättslig grund för att få behandla personuppgifter vilket samtliga organisationer också arbetar med att uppfylla. Övriga åtgärder varierar mellan organisationerna. Åtgärdernas omfattning varierar utifrån hur väl organisationerna tidigare har följt personuppgiftslagen.

### 7.2 Vilka utmaningar finns samt vilka åtgärder har organisationer vidtagit för att följa dataskyddsförordningen gällande personuppgiftsbehandlingen?

Det som är generellt för alla organisationer i studien är att de arbetat aktivt för att få en god kunskap om dataskyddsförordningen och vad den innefattar. Det finns även en god förståelse för vilka konsekvenser det kan innebära i form av sanktioner för respektive organisation vid försummelse av regel i dataskyddsförordning.

Det har genomgående utarbetats rutiner och planer för vilka åtgärder som bör genomföras gällande organisationernas personuppgiftsbehandling. Det har praktiskt inneburit svårigheter att infria de rutiner och planer som organisationerna utformat för att uppfylla dataskyddsförordningens regler. Detta eftersom att IT-verktyg generellt saknas i den utsträckning som behövs för att hantera dessa kvantiteter av personuppgifter.

### 7.3 Kunskapsbidrag

Denna studie bidrar till ökad kunskap och förståelse för vilka utmaningar organisationerna ställs inför samt vilka åtgärder som vidtagit för att följa dataskyddsförordningens regler. Vad som framkommit i denna studie är att organisationerna har problem att hantera ostrukturerade personuppgifter. Vi kan därför uppmana systemutvecklare att ha den personliga integriteten i beaktning vid framtagandet av IT-verktyg. Detta för att undvika problem som kan uppstå vid behandlingen av personuppgifter. Organisationerna har upplevt utmaningar i att presentera avtals- och samtyckestexter i avsikt att den registrerade ska förstå innebörden av dess personuppgiftsbehandling. Vi kan med detta uppmana interaktionsdesigners att utveckla flöden för hur avtals- och samtyckestexter ska visas i

olika e-tjänster. Slutligen visar studien att organisationerna har fått bättre självkännedom om sina IT-system och dess behandling av personuppgifter i samband med dataskyddsförordningen.

## 7.4 Förslag på vidare forskning

Denna studie kan ses som ett underlag för framtida forskning. Det skulle enligt oss vara intressant att se hur utmaningar och åtgärder ser ut i framtiden hos organisationer när dataskyddsförordningen trätt i kraft. Ytterligare ett förslag på vidare forskning är att undersöka hur Datainspektionen valt att utöva tillsyn mot organisationer samt hur Datainspektionen kommer att bedöma dessa organisationers vidtagna åtgärder.

## 8 Epilog

*I det här kapitlet beskrivs vad vi författare tror om ämnet i framtiden.*

I framtiden tror vi att Datainspektionen kommer att spela en stor roll i hur organisationer kommer att tillämpa dataskyddsförordningens regler. Innan Datainspektionen utdömt några sanktionsavgifter är det svårt att säga vilka åtgärder organisationerna bör vidta och se som de mest kritiska. Organisationer arbetar idag med att åtgärda utmaningar som har kommit uppstå i omställningen till dataskyddsförordningen. Detta handlar till största del om att personuppgiftslagen inte tidigare har tillämpats.

Ifall organisationers behandling av personuppgifter stämmer överens med vad som uttrycks i dess samtyckestexter är svårt för oss att svara på. Det kommer vara upp till Datainspektionen att granska om behandlingen stämmer överens med vad organisationerna uppger i sina samtyckestexter.

Vi tror även att utvecklare i framtiden kommer att kunna dra ekonomiska fördelar tack vare de behov som uppstår i och med införandet av dataskyddsförordningen. Dessa behov kommer att innefatta nyutveckling och förvaltning av IT-system. Genom att beakta dataskyddsförordningens regler när IT-system utvecklas och förvaltas uppstår en ny marknad och utvecklare kan på så sätt dra fördelar av införandet.

Det har månaderna innan införandet av dataskyddsförordningen och veckorna efter skickats ut mängder av mail från organisationer till privatpersoner. Dessa mail innefattar information om dataskyddsförordningen, inhämtandet av nya samtycken med mera. Det står i vissa mail att *"dina personuppgifter kommer att raderas om du inte ger ditt samtycke"*. För att veta om personuppgifterna kommer att raderas om ett samtycke inte har inhämtats är svårt för oss att svara på. Det kommer återigen vara upp till Datainspektionen att granska om de personuppgifter organisationerna uppger ska raderas också gör det.

Vi tror att vissa organisationer kommer att hitta "kryphål" för att undanhålla information från den registrerade och på så sätt fortsätta med behandlingen av personuppgifter trots att ingen rättslig grund finns. Vi tror att personuppgifter kommer att kunna klassificeras utan att kunna kopplas till en fysisk person vid en granskning av Datainspektionen. Detta tror vi kan medföra en annan typ av marknadsföring och målgruppsanpassning utifrån nya statistiska metoder med personuppgifter som underlag. Den information som genererats utifrån personuppgifter kommer att inneha ett högre värde än de personuppgifter som behandlas. Vissa organisationer kommer eventuellt bygga IT-system som behandlar data och som sedan kan kopplas samman för att generera personuppgifter vid behov. Införandet av dataskyddsförordningen kan resultera i konsekvenser för den personliga integriteten då organisationer fortsatt vill utnyttja personuppgifter för att få marknadsmässiga fördelar.

Vi tror att nya roller och kompetenser kommer att behöva tillsättas då ett större fokus kommer att ägnas åt dataskydd. Det kommer troligtvis behöva tillsättas fler IT-jurister som besitter specialkunskaper och kan tillämpa lagtext praktiskt i tekniken. Detta för att värna om den personliga integriteten och skydda organisationer från lagöverträdelse.

## Källförteckning

Appelgren, E., Journalistik, Institutionen för samhällsvetenskaper, & Södertörns högskola. (2017). The reasons behind tracing audience behavior: A matter of paternalism and transparency. *International Journal of Communication (Online)*, 11, 2178

Bhaimia, S. (2018). The general data protection regulation: The next generation of EU data protection. *Legal Information Management*, 18(1), 21.  
doi:10.1017/S1472669618000051

Björklund, M. & Paulsson, U. (2003). *Seminarieboken: att skriva, presentera och opponera*. Lund: Studentlitteratur.

Datainspektionen. (2017). *Dataskyddsförordningen*. Hämtad 2018-04-04, från <https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/>

Datainspektionen. (u.å.). *Personuppgiftslagen*. Hämtad 2018-04-04, från <https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/>

Europaparlamentets och rådets förordning (EU) 2016/679. Tillgänglig: <http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=>

European Parliament. (2007). *Guidelines on Consent under Regulation 2016/679*. European Parliament

Gilmore, R. O. (2016). From big data to deep insight in developmental science: Big data in development. *Wiley Interdisciplinary Reviews: Cognitive Science*, 7(2), 112-126.  
doi:10.1002/wcs.1379

Jerkert, J. (u.å.). peer review. I *Nationalencyklopedin*. Tillgänglig: <https://www-ne-se.www.bibproxy.du.se/uppslagsverk/encyklopedi/l%C3%A5ng/peer-review>

Jørgensen, R. F., & Desai, T. (2017). Right to privacy meets online platforms: Exploring privacy complaints against facebook and google. *Nordic Journal of Human Rights*, 35(2), 106. doi:10.1080/18918131.2017.1314110

Koskelainen, A. (2018, 23 maj). Datainspektionens jätteblunder: det går inte längre att hitta GDPR-informationen. IDG.se. Hämtad 2018-05-30, från <https://computersweden.idg.se/2.2683/1.702956/gdpr-datainspektionen>

Malmqvist, M. (2018, 9 april). GDPR-chock väntar småföretagen – inte ens hälften har börjat anpassa sig. IDG.se. Hämtad 2018-04-13, från <https://computersweden.idg.se/2.2683/1.700510/smaforetag-gdpr?queryText=gdpr>

Noain-Sánchez, A. (2016). "Privacy by default" and active "informed consent" by layers. *Journal of Information, Communication & Ethics in Society*, 14(2), 124-138. Retrieved from <http://www.du.se.proxy.aspx/login?url=http://search.proquest.com/?url=https://search.proquest.com/docview/1823117425?accountid=10404>

Oates, B. J. (2006) *Researching information systems and computing*. London: SAGE Publications.

Patel, R., & Davidson, B. (2003). *Forskningsmetodikens grunder – att planera, genomföra och rapportera en undersökning*, tredje upplagan, Lund: Studentlitteratur.

Rotenberg, M., & Jacobs, D. (2013). Updating the law of information privacy: The new framework of the european union. *Harvard Journal of Law & Public Policy*, 36(2), 605.

Zuiderveen Borgesius, F., & Poort, J. (2017). Online price discrimination and EU data privacy law. *Journal of Consumer Policy*, 40(3), 347-366.  
doi:<http://dx.doi.org/10.1007/s10603-017-9354-z>

# Bilagor

## Bilaga 1 – Intervjuguide

**Inledning.** Den 25 maj (2018) träder dataskyddsförordningen i kraft. Många organisationer har med det tvingats omformulera sina samtyckestexter samt sin behandling av personuppgifter för att upprätthålla förordningens regler. Med samtyckestexter menar vi: policy, villkor, avtal eller liknande som den registrerade (användaren) förbinder sig till vid medgivande.

1. Hur ser ni på införandet av dataskyddsförordningen inom er organisation?
2. Krävs det stora omställningar i era nuvarande samtyckestexter (enl. PuL) för att upprätthålla dataskyddsförordningens regler och vilka utmaningar ser ni i dessa omställningar?
3. Krävs det stora omställningar i er nuvarande personuppgiftsbehandling (IT-system) för att upprätthålla dataskyddsförordningens regler och vilka utmaningar ser ni i dessa omställningar?
4. Kommer ert syfte vid behandlingen av personuppgifter att förändras i omställningen till den nya dataskyddsförordningen och dess förändrade riktlinjer för samtycke?
5. Kommer era nya samtyckestexter (enl. dataskyddsförordningen) att överensstämma med hur ni i praktiken kommer att behandla personuppgifter eller vilka åtgärder måste ni vidta för att dessa ska stämma överens?
6. Vilka åtgärder har vidtagits vid framtagandet av samtyckestexter (enl. dataskyddsförordningen) för att det ska vara så informativt som möjligt för den registrerade?
7. Är era nya samtyckestexter (enl. dataskyddsförordningen) tillräckligt informativa för att den registrerade ska kunna fatta ett avgörande beslut i fråga att ingå avtal?

## Bilaga 2 - Informationsbrev till intervjuperson

Hej, vi är två studenter vid Högskolan Dalarna som studerar Systemvetenskapliga programmet. Vi ska nu genomföra vårt examensarbete i Informatik. För att nå ett så bra resultat som möjligt i vår studie skulle vi vara mycket tacksamma om ni har möjligheten att delta i en intervju. Studien behandlar den nya dataskyddsförordningen och dess samtycke.

Syftet med den här studien är att identifiera hur ett antal organisationer har omformulerat sina samtycken för att möta omställningen till dataskyddsförordningen. Med detta vill vi klargöra vilka åtgärder som vidtagits för att följa dataskyddsförordningens regler.

Vi hoppas med denna studie kunna bidra med ökad kunskap i hur organisationer valt att genomföra omställningen gällande samtycke i enlighet med dataskyddsförordningens regler. Med detta vill vi ge svar på: om åtgärder vidtagits, vilka åtgärder som vidtagits och hur man valt att gå tillväga för att vidta dessa åtgärder.

- Du som intervjudeltagare får när som helst avbryta medverkan i denna intervju utan att ange orsak om så önskas.
- Intervjun kommer att genomföras av två intervjuledare om inte du som intervjudeltagaren endast vill att en intervjuledare finns närvarande.
- Platsen för intervjun kan anpassas utifrån vad som är mest lämpligt för dig som intervjuperson eller i samråd med intervjuledarna. Om ett fysiskt möte inte är möjligt kan även ett/flera telefon- eller Skype samtal vara ett alternativ till intervju.
- Intervjun kommer att spelas in (inspelningsutrustning, ex. mobiltelefon) för att underlätta transkribering och sammanställning av intervjutillfället. Ljudfilen kommer efter transkribering att raderas.
- Du som intervjuperson (representant av en organisation) kommer inte att nämnas vid namn i studien (i enlighet med Codex). Du utlovas full anonymitet och kommer att avidentifieras.
- Innan publicering kommer du som intervjuperson att ges möjlighet till granskning av studien och alternativt ge invändningar på materialet.
- Efter ditt godkännande kommer studien att lämnas in till examinator (Högskolan Dalarna) för bedömning. Godkända studier (rapporter) publiceras i Diva (Ett digitalt vetenskapligt arkiv).

Vi vore tacksamma om ni vill delta i denna studie genom en intervju. Intervjun uppskattas i effektiv tid ta 30–45 minuter att genomföra.

*Med vänliga hälsningar,*

### **Kontaktuppgifter**

Tesfaom Alem | h15tesal@du.se | 072-933 33 63  
William Lind | h13willi@du.se | 076-829 38 58

Handledare: Johan Håkansson (Univ lektor kulturgeografi, Informatik)  
jhk@du.se | 023-77 85 73

Högskolan Dalarna – SE-791 88 Falun – Tel 023-77 80 00



## Bilaga 3 - Blankett för Etikprövning

		Ja	Tveksam	Nej
1	Kan frivilligheten att delta i studien ifrågasättas, d.v.s. innehåller studien t.ex. barn, personer med nedsatt kognitiv förmåga, personer med psykiska funktionshinder samt personer i beroendeställning i förhållande till den som utför studien (ex. på personer i beroendeställning är patienter eller elever)?			X
2	Innebär undersökningen att informerat samtycke inte kommer att inhämtas (d.v.s. forskningspersonerna kommer inte att få full information om undersökningen och/eller möjlighet att avsäga sig ett deltagande)?			X
3	Innebär undersökningen någon form av fysiskt ingrepp på forskningspersonerna?			X
4	Kan undersökningen påverka forskningspersonerna fysiskt eller psykiskt (t.ex. väcka traumatiska minnen till liv)?			X
5	Används biologiskt material som kan härledas till en levande eller avliden människa (t.ex. blodprov)?			X
6	<p>Avser undersökningen att behandla känsliga personuppgifter?</p> <p>Med känsliga personuppgifter avses, enligt Personuppgiftslagen, uppgifter som berör:</p> <ul style="list-style-type: none"> <li>• hälsa eller sexualliv</li> <li>• etniskt ursprung</li> <li>• politiska åsikter</li> <li>• religiös eller filosofisk övertygelse</li> <li>• medlemskap i fackförening</li> </ul>			X