Examensarbete, Högskolan på Åland,
Utbildningsprogrammet för företagsekonomi

GDPR i praktiken

Arnel Kahrimanovic, Selma Mesic

2020:15

Datum för godkännande: 13.05.2020
Handledare: Christer Kullman

EXAMENSARBETE
Högskolan på Åland

Utbildningsprogram:	Företagsekonomi
Författare:	Arnel Kahrimanovic, Selma Mesic
Arbetets namn:	GDPR i praktiken
Handledare:	Christer Kullman
Uppdragsgivare:	Högskolan på Åland

Abstrakt

Till följd av den nya tekniska utvecklingen kom dataskyddsförordningen mer känd som GDPR.

Regelverket togs i bruk den 25 maj 2018 med syfte att förstärka kontrollen för privatpersoners uppgifter eftersom EU inte längre kunde garantera sina medborgares rättigheter i den snabba växande värld. GDPR kommer med nya bestämmelser över hur personuppgifter skall behandlas samt medför högre krav på hantering av personuppgifter. Organisationerna som inte följer GDPR kan riskera betala en administrativ sanktionsavgift om behandlingen inte utförs i enlighet med förordningen.

Syftet med den här examensarbete är att genom kvalitativ intervjustudie undersöka vad organisationerna på Åland har gjort för att uppfylla de nya kraven samt vilka åtgärder dem har vidtagit.

Resultatet visar att organisationerna har vidtagit nya tekniska och organisatoriska säkerhetsåtgärder för att deras kunder skall känna sig trygga och att deras insamlade personuppgifter ska behandlas säkert enligt lagen.
Kommunikation och informationsutbyte med kunden har även ökat.

Nyckelord (sökord)
GDPR, dataskyddsförordningen, personuppgifter, organisation, anpassning

Högskolans serienummer:	**ISSN:**	**Språk:**	**Sidantal:**
2020:15	1458–1531	Svenska	41 sidor

Inlämningsdatum:	**Presentationsdatum:**	**Datum för godkännande:**
08.05.2020	13.05.2020	13.05.2020

DEGREE THESIS
Åland University of Applied Sciences

Study program:	Business Administration
Author:	Arnel Kahrimanovic, Selma Mesic
Title:	GDPR in Practice
Academic Supervisor:	Christer Kullman
Technical Supervisor:	Aland University of Applied Sciences

Abstract

As a result of the new technological development, the Data Protection Regulation (GDPR) law was introduced.

The regulations were put into operation on May 25, 2018 with the aim of strengthening the control of private information, as the EU could no longer guarantee the rights of its citizens in the fast growing world. The GDPR law introduces new rules on personal data and imposed higher demands how the personal data should be processed. Organizations that do not comply with the GDPR may be liable to pay an administrative penalty fee if the treatment is not performed in accordance with the new regulation.

The purpose of this thesis is to through a qualitative interview investigate what the organizations in Aland have done so far and what new requirements and the measures they have taken.

The result shows that the organizations have taken new technical and organizational security measures, in order for their customers to feel confident that their personal data will be processed securely and in accordance with the new EU law.
Communication and exchange of information with the customer has also increased.

Keywords

GDPR, data protection regulation, data management, organization, adaptation

Serial number:	ISSN:	Language:	Number of pages:
2020:15	1458–1531	Swedish	41 pages

Handed in:	Date of presentation:	Approved on:
08.05.2020	13.05.2020	13.05.2020

INNEHÅLLSFÖRTECKNING

FIGURFÖRTECKNING

1 INLEDNING

1.1 Bakgrund

När det gäller skydd av personuppgifter har den snabba tekniska utvecklingen och globaliseringen skapat nya utmaningar och stora förändringar. Idag kan vi se att allt fler personer runt om i världen som gör sina personuppgifter allmänt tillgängliga i allt större omfattning. Delning och insamling av personuppgifter har ökat och det har aldrig varit så lätt att sprida uppgifterna som idag (Europeiska unionens officiella tidning, 2016, s. 2). Individens integritet rubbas ständigt och det blir större risk att utsättas för intrång, därför är det viktigt att genomföra lämpliga skyddsåtgärder (Fridlinger, 2018, ss. 16-17).

Till följd av den nya utvecklingen kom dataskyddsförordningen mer känd som GDRP (General Data Protection Regulation) som började tillämpas som lag den 25 maj 2018. Den nya europeiska allmänna förordningen antogs i syfte att förstärka kontrollen av personlig information för privatpersoner (Wetterberg, 2019).

Bakgrund till förordningen: *”Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet.”*och*” Skyddet för människor bör, oavsett deras medborgarskap eller hemvist respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd för personuppgifter.”* (Europeiska unionens officiella tidning, 2016, s. 1)

Förordningen ersätter EU:s dataskyddsdirektiv från 1995 och de nationella reglerna, såsom den åländska personuppgiftslagen (LL om behandling av personuppgifter) (Datainspektionen Åland, 2018). Tidigare har Åland följt det gamla EU-direktivet. Detta direktiv om behandling av personuppgifter har inte ändrats nästan i 15 år (Ålands lagting, 2018). Under denna period har tekniken gjort stora framsteg och det finns en större risk för stöld av personuppgifter och större behov av att skydda dem.

Allmänna dataskyddsförordningen för skydd av personuppgifter är en ny europeisk förordning som medför många och strängare ändringar i personuppgifter och hur de får användas. Till skillnad från tidigare personuppgiftslagen är GDPR en direkt tillämplig för

EU:s medlemsstater. För organisationer och företag innebär det att de måste se till att deras arbetsrutiner inte på något sätt går emot GDPR och att de uppfyller reglerna då det gäller behandling av personuppgifter, annars riskerar de betala en administrativ sanktionsavgift. Sanktionsavgiften kan vara upp till 20 miljoner euro eller fyra procent av den globala årsomsättningen. (Datainspektion, u.d.)

1.2 Syfte och frågeställning

Detta examensarbete ger större förståelse om den nya dataskyddsförordningen GDPR och hur den har påverkat organisationerna på Åland. Huvudsyfte med detta examensarbete är att genom kvalitativ intervjustudie undersöka vad dem har gjort för att anpassa sig till den nya förordningen, som trädde i kraft den 24 maj 2016 och började tillämpas den 25 maj 2018. Arbetet syftar till att ta reda på hur åländska organisationer har anpassat sig till det nya regelverket och vilka var de största förändringar för dem, med hjälp av nedanstående frågeställningar.

- Vilka konkreta åtgärder har de åländska företag vidtagit?
- Vilka nya arbetsprocesser och rutiner har tagits i bruk?

1.3 Avgränsningar

För att utreda ovanstående frågeställningar kommer vi att undersöka tre organisationer på Åland som har den dagliga hantering och lagring av personuppgifter. Vi valde att vårt uppsatshuvudfokus skall ligga på att undersöka förändringar som GDPR har medfört på de åländska organisationer samt hur dem har anpassat sig efter dem.

Vi kommer inte att undersöka hur den nya lagen har påverkat privatpersoner utan endast fokusera på hur organisationerna ställer sig till den nya lagen och vad de gjort för att anpassa sig. Detta arbete kommer endast att fokusera på den nya dataskyddsförordningen och vi kommer inte göra någon jämförelse mellan den gamla personuppgiftslagen och den nya dataskyddsförordningen.

Examensarbetet kommer mest handla om hur organisationerna har anpassat sig efter att GDPR har trätt i kraft. Vi kommer även lite att gå in på förberedelserna innan regelverket trädde i kraft, eftersom alla företag, myndigheter, föreningar etc. som behandlar personuppgifter har haft en lång tid att anpassa sig till det nya regelverket i och med att övergångsperioden var i två år.

2 TEORI

2.1 Den allmänna dataskyddsförordningen GDPR

Förordningens fullständiga namn är General Data Protection Regulation, förkortat GDPR som är en ny förordning inom Europeiska Unionen med syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter. GDPR är direkt tillämpad lagstiftning som gäller alla medlemsländer. Istället för att varje land tillämpar egna dataskyddslagar, så styrs nu hela EU av en gemensam förordning (Äldrecentrum, 2018). Syften med GDPR var att modernisera och uppdatera principer av EU:s dataskyddsdirektivet 95/46/EG samt anpassa sig till den nya digitala världen (Datainspektionen, u.d.).

”Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/ EG.” (Europeiska unionens officiella tidning, 2016, s. 1)

Skillnaden mellan förordning och direktiv förklaras nedan:

En EU-förordning gäller direkt till alla medlemsstater och kräver inte att nationella lagar skapas. Alla medlemsländer har rätten att skapa enskilda nationella lagar, som preciserar och kompletterar förordningen, utan att strida mot den (Eduskunta riksdagen, 2018). Till skillnad från en EU-förordning måste ett EU-direktiv göras om till en nationell lagstiftning och det är upp till varje medlemsstat att implementera regelverket och tolka av det (Europeiska kommissionen, u.d.). Den nya landskapslagen (2019:9) om dataskydd inom landskaps- och kommunalförvaltningen ersätter den gamla åländska landskapslagen (2007:88) som kompletterar GDPR nu (Ålands Landskapsregering, 2019).

”Genom denna lag preciseras och kompletteras tillämpningen på Åland av Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, nedan dataskyddsförordningen.” (Ålands landskapsregering, 2019)

2.1.1 Definition av personuppgifter

Det centrala i hela GDPR förordningen är begreppet personuppgift. Dataskyddsförordningen tillämpas endast om den behandlade data innehåller personuppgifter (Fridlinger, 2018, s. 44).

GDPR:s juridiska förklaring på personuppgift definieras i Artikel 4 i GDPR på följande sätt:

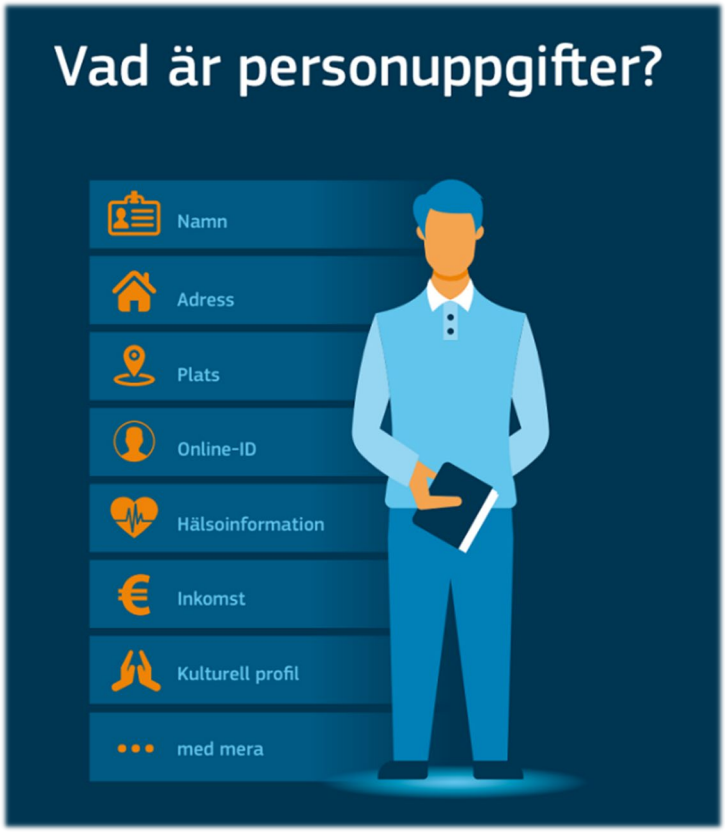
”Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.” (Europeiska unionens officiella tidning, 2016, s. 33)

Den behandlade data av personuppgifter kan vara allt från namn, personnummer, adresser till fotografier, ljudklipp, så länge det kan kopplas till en fysisk person som är i livet. Dataskyddsförordningen gäller enbart behandling av personuppgifter som är knutna till levande personer. Uppgifter om avlidna räknas inte som personuppgifter.
En personuppgift handlar alltid om uppgifter som kan direkt eller indirekt identifiera en fysisk person (Fridlinger, 2018, ss. 44-45).

Direkta uppgifter innebär personuppgifter som kan ensamt identifiera en person, till exempel personnummer. Till den indirekta identifieringen räknas en kombination av en enskild uppgift med en annan uppgift som leder till en levande person (Wetterberg, 2019, s. 35).

En speciell kategori av personuppgifter kallas känsliga personuppgifter. Med känsliga personuppgifter menas personuppgifter som avslöjar ras eller personens etniska ursprung, politiska åsikter, religionsåskådning eller sexuella läggning (Fridlinger, 2018, s. 45). Även uppgifter om personens hälsa klassas som känsliga. Hälsouppgifter räknas som en särskild kategori känsliga personuppgifter i dataskyddsförordningen och det är särskilda regler som gäller för behandling av sådana uppgifter (Wetterberg, 2019, s. 41).

Figur 1 visar några exempel på personuppgifter:



Figur 1 – Illustration på vanliga och känsliga personuppgifter (Samlogic, u.d.)

2.1.2 Begreppet behandling

Dataskyddsförordningen är tillämplig på all behandling av personuppgifter, vilket betyder efter att man har säkerställt den insamlade data som rör sig om en personuppgift, är nästa kriterium att dataskyddsförordningen skall vara tillämplig dvs. det skall röra sig om en behandling som förklaras nedan. (Fridlinger, 2018, s. 46).

GDPR:s juridiska förklaring på personuppgiftsbehandling definieras i Artikel 4 i GDPR på följande sätt:

”En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på

annat sätt, justering eller sammanförande, begränsning, radering eller förstöring." (Fridlinger, 2018, s. 46)

För att GDPR ska vara tillämplig krävs vidare att behandlingen skall ske på helt eller delvis automatiserad sätt. Exempel på behandling som sker på automatiskt sätt är då det rör sig om personuppgifter i dataformat. En delvis automatiserad behandling är när personuppgifterna samlas in manuellt för att sedan registreras i datorformat. GDPR gäller också för manuell behandling, när personuppgifterna samlas in i pappersformat och skall vara sökbart enligt särskilda kriterier. Handlar det om manuell behandling så skall personuppgifterna ingå i ett register (Datainspektionen, u.d.).

Som framgår i ovanstående definition är begreppet behandling allt från t.ex. insamling, bearbetning, ändring, användning, organisering, läsning, överföring, radering m.m.

Profilering och pseudonymisering räknas som speciella typer av behandling. Dataskyddsförordningens definition på profilering är följande:

"Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar." (Europeiska unionens officiella tidning, 2016, s. Art. 4.4)

Profilering av personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person särskilt för att analysera eller förutsäga exempelvis dennes arbetsprestation, ekonomiska situation eller personliga preferenser.

Pseudonymisering är även ett centralt begrepp inom behandling. Pseudonymisering är en teknik för anonymisering som gör det lättare att hantera personuppgifter på ett säkrare sätt. Vilket innebär att personuppgifter lagras skilda från övriga personuppgifter (Multisoft, u.d.).

"Dataskyddsförordningen definierar det som en behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att

kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person."
(Europeiska unionens officiella tidning, 2016, s. Art.4.5)

2.2 Grundläggande principer för behandlingen av personuppgifter

I det officiella GDPR-dokumentet i Artikel 5 finner man ett antal samlade grundläggande principer som anses vara kärnan i dataskyddsförordningen. Principerna gäller för all behandling av personuppgifter och det är viktigt att alla organisationer tillämpar dem (Wetterberg, 2019, s. 50).

• *Laglighet, Korrekthet och Öppenhet*
Den första principen innebär att det måste finnas en rättslig grund för behandlingen av personuppgifter. Vilka rättsliga grunder som finns för behandling av personuppgifter kommer vi att ta upp i nästa rubrik. Med denna princip menas vidare att personuppgifter ska behandlas på ett korrekt och öppet sätt i relation till den person som behandlas (den registrerade).
För den registrerade ska det vara klart och tydligt hur personuppgifter som rör han eller hon behandlas och på samma sätt ska information vara kortfattad, lättbegriplig samt utformad på ett tydligt och enkelt språk som är lätt att förstå. (Di.ax, u.d.)

• *Ändamålsbegränsning*
När ett företag eller organisation samlar in personuppgifter måste de vara säkra vad de ska användas till från början och förmedla det till den registrerade. Ändamålet skall vara tydlig innan personuppgifterna samlas in. Insamling av personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålet får inte ändras i efterhand utan att den berörda personen har fått information om detta. Från denna huvudregel kan göras undantag där det är godtaget att använda de insamlade uppgifterna till ett annat ändamål, bara om dessa är förenliga med de ursprungliga ändamålen, och de registrerade måste i så fall också informeras om detta. (Di.ax, u.d.)

• *Uppgiftsminimering*

Insamling av personuppgifter måste vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål vad de ska användas till. Det innebär att personuppgiftsansvarige inte ska samla in uppgifter för obestämda framtida behov, som dem inte egentligen behöver. (Di.ax, u.d.)

• *Korrekthet*

De registrerade personuppgifterna ska vara korrekta och uppdaterade. Den som behandlar personuppgifter har ett ansvar att vidta rimliga åtgärder för att säkerställa att personuppgifterna som är felaktiga rättas eller raderas utan dröjsmål. (Di.ax, u.d.)

• *Lagringsminimering*

Personuppgifterna skall inte sparas under längre tid än vad som är nödvändigt för ändamålet. Det är viktigt att ha rutiner och full kontroll över gallring av personuppgifter. De personuppgifter som inte längre behövs ska raderas eller avidentifieras efter en viss tid. (Di.ax, u.d.)

• *Integritet och konfidentialitet*

Företaget som behandlar personuppgifterna ska skydda dem, så att ingen obehörig kommer åt dem eller så att de inte behandlas på ett otillåtet sätt. De ska även skyddas mot förlust och skada. Därför är det viktigt att vidta lämpliga säkerhetsåtgärder såsom tekniska och organisatoriska. Ett exempel på tekniska åtgärder kan vara pseudonymisering som vi tidigare nämnde i arbetet. Till de organisatoriska åtgärderna hör riktlinjer, instruktioner och rutiner. (Di.ax, u.d.)

• *Ansvarsskyldighet*

Principen om ansvarsskyldighet innebär personuppgiftsansvariga har ansvar över att se till att de 6 ovanstående principerna följs i verksamheten. Företaget skall också kunna bevisa att principerna efterlevs och att dem uppfyller tekniska och organisatoriska åtgärder. (Di.ax, u.d.)

2.3 Rättslig grund för behandling av personuppgifter

För att en personuppgiftsbehandling ska vara laglig måste de sex olika rättsliga grunder som anges i det officiella GDPR-dokumentet följas. Behandling av personuppgifter får endast ske under de omständigheter som lyfts fram i lagstiftningen. Personuppgiftsansvarige ska kunna dokumentera varför lagring av personuppgifter är laglig. Personuppgiftsbehandlingen är inte laglig om en rättslig grund saknas (Europeiska Kommisionen, u.d.). De viktigaste rättsliga grunderna som en organisation kan använda nämns nedan.

2.3.1 Samtycke

Företaget måste få personens samtycke till hanteringen av personuppgifter. För att ett samtycke skall vara giltig skall den som behandlar personuppgifter följa nedanstående villkor.

”Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.” (Datainspektionen, u.d.)

Ett samtycke räknas inte som giltig om det inte sker frivilligt. Personen skall ha ett fritt val. Hen skall kunna tacka nej också utan att det får negativa konsekvenser.

Enligt datainspektionen skall det vara lika lätt att lämna ett samtycke som att återkalla det. Vilket innebär att ett samtycke bär också rättigheten att när som helst kunna dras tillbaka. Personen skall också få information om vad personuppgiftsbehandlingen innebär. Sådant samtycke brukar kallas informerat samtycke. Den som ska samtycka måste få veta i förväg vad det är den samtycke samt syfte med insamlingen av personuppgifterna (Datainspektionen, u.d.).

Företaget skall komma ihåg när personen har samtyckt till att hans eller hennes personuppgifter behandlas, får de bara behandla uppgifterna för de ändamål som samtycket lämnades för. Om behandlingen tjänar flera olika syften måste det som regel vara möjligt att ge separata samtycke för varje område. Samtycke skall ges frivilligt och aktivt på ett uttryckligt sätt. Detta innebär att berörda personen måste uttryckligen kryssa i rutan eller genom en signatur i ett formulär (Europeiska unionens officiella tidning, 2016, s. Skäl 32).

Personuppgiftsansvarige skall använda tydligt och enkelt språk vid kommunikation med de registrerade, som är lätt att förstå (Europeiska unionens officiella tidning, 2016, s. Art.7).

2.3.2 Andra rättsliga grunder för behandling

Organisationerna kan också stödja personuppgiftsbehandling på någon av de andra fem rättsliga grunderna. Den officiella tidningen GDPR listar fram fem villkor upp där samtycken inte behövs för behandling av personuppgifter. Det innebär att de rättslig grund utan ett samtycke. De två sista rättsliga grunderna är främst avsedda för myndigheter, forskningsinstitutioner mm.

1. Det första villkoret är då personuppgiftsansvarige har ett avtal med den registrerade personen eller ska ingå ett avtal. Exempel på sådan behandling kan vara när ett företag identifierar den berörda personen som kund och för att kunna hantera och leverera tjänster som hen har beställt. Samt insamling av personuppgifter som krävs för att hantera fakturering och betalning (Datainspektionen, u.d.).
2. Det andra villkoret är rättslig förpliktelse. Detta innebär att företaget behandlar personuppgifter enligt lagar och regler som gäller för verksamheten. Ett vanligt exempel på rättslig förpliktelse är bokföringsskyldigheten som anges i bokföringslagen (Datainspektionen, u.d.).

3. Det tredje är intresseavvägning när orsaken till att företaget behandlar personuppgifter vägrar tyngre än den registrerades integritet och då behandlingen är nödvändig för det aktuella ändamålet. Detta innebär att företaget får behandla den registrerades personuppgifter utan den registrerades samtycke. Ett exempel på intresseavvägning är när företaget använder sig av marknadsföring och direktreklam. Företaget får inte skicka direktreklam om den registrerade har sagt nej till det (Datainspektionen, u.d.).

4. De rättsliga grunderna som myndighetsutövning och uppgift av allmänt intresse är tillåtet endast om syftet med behandlingen är nödvändig för att utföra uppgiften som ett led i myndighetsutövning eller allmänt intresse. Ett exempel på det är betygsättning för att

utbilda och forska. Dessa rättsliga grunder är relevant för myndigheter och är vanlig inom högskolan (Högskolan i Borås, 2019).

5. Den sista rättsliga grunden är skydd av grundläggande intresse och används mest då människornas liv är hotande. Den personuppgiftsansvarige får endast behandla personuppgifter om det är nödvändigt för att rädda den registrerades eller någon annan persons liv. Ett exempel på det här är då personen är medvetslös och kan inte själv lämna samtycke. Den här rättsliga grunden skall man helst undvika om det går att lösa situationen på att annat sätt dvs. om den registrerade kan själv fatta beslut skall personuppgiftsansvarige välja en annan rättslig grund (Dataskydsinspektionen, u.d.).

2.4 Personuppgiftsansvarig och personuppgiftsbiträde

Ett av syftena i GDPR är att tydligt klargöra vilka skyldigheter och rättigheter de olika rollerna som behandlar personuppgifter har (Europeiska unionens officiella tidning, 2016, s. Skäl 11). Enligt Dataskyddsförordningen GDPR, behöver organisationer förstå skillnaden mellan begreppen personuppgiftsansvarig och personuppgiftsbiträde.

Dataskyddsförordningens två roller för behandling av personuppgifter är personuppgiftsansvarig, art. 24 och 26, eller personuppgiftsbiträde, art. 28. GDPR sätter skyldigheter och begränsningar vem som är ansvarig för vad, beroende på vilken typ din verksamhet faller under (GDPR Grunder: Skillnad, 2018).

Personuppgiftsansvarig är den *”som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.”* (Europeiska unionens officiella tidning, 2016, s. Art 4.7)
Personuppgiftsbiträde är den *”som behandlar personuppgifter för den personuppgiftsansvariges räkning.”* (Europeiska unionens officiella tidning, 2016, s. Art 4.8)

GDPR:s juridiska förklaring på personuppgiftsansvarig definieras i GDPR på följande sätt:

”En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt.” (Europeiska unionens officiella tidning, 2016, s. Art. 4)

Den personuppgiftsansvarige är ett företag eller organisation som fastställer för vilka ändamål personuppgifter behandlas och genom vilka medel. Den skall bestämma varför personuppgifter behandlas och hur behandlingen ska gå till. Med medel avses tekniska och organisatoriska åtgärder som avgör hur själva behandlingen skall gå till (Wetterberg, 2019, s. 53). Enligt GDPR skall varje personuppgiftsansvarig föra register över behandlingen som sker under dennes ansvar som ska innehålla kontaktuppgifter, ändamålsbeskrivning för behandlingen, kategorisering av registrerade och av personuppgifter (Europeiska unionens officiella tidning, 2016, s. Art.30).

Ett företag eller en organisation kan också vara gemensamt personuppgiftsansvarig. Om det är flera som är personuppgiftsansvariga ska de gemensamt bestämma ”varför” och ”hur” personuppgifter ska behandlas. I detta fall måste ett avtal ingås där båda parternas ansvar lyfts fram för att fullgöra sina skyldigheter enligt förordningen. Det föreligger ett solidariskt ansvar dem emellan. (Europesika Kommissionen, u.d.)

Ett exempel på gemensamt personuppgiftsansvarig är då ett företag säljer en tjänst online men anlitar ett annat företag som erbjuder någon form av tilläggstjänst i samband med det. Till exempel betaltjänster och paketförmedlingsföretag. Att ha en situation där flera aktörer är involverade är ganska vanligt, där det ibland är svårt att bestämma rollerna vem som är personuppgiftsansvarig eller om de har ett gemensamt ansvar (Fridlinger, 2018, s. 54). GDPR:s juridiska förklaring på personuppgiftsbiträde definieras även på följande sätt:

”En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.” (Europeiska unionens officiella tidning, 2016, s. Art. 4)

Ett personuppgiftsbiträde är en fysisk eller juridisk person, ofta en tredje part som är utsedd av den personuppgiftsansvarige att hantera den personuppgiftsansvariges data enligt de givna riktlinjerna. Företaget som behandlar data åt den personuppgiftsansvariges vägnar kallas alltså personuppgiftsbiträden (Europeiska unionens officiella tidning, 2016, s. art 4.8).

Ett bra exempel på ett personuppgiftsbiträde är ett lönehanteringsföretag för betalning av lönerna. Personuppgiftsbiträde sköter då utbetalning av löner och andra relaterade löneuppgifter för ett annat företag. Det betyder att företaget eller organisation som har anlitat lönehanteringsföretaget fastställer varför personuppgifter behandlas och hur själva behandlingen ska gå till och är därmed personuppgiftsansvarig.
Lönehanteringsföretaget som hanterar personuppgifterna på personuppgiftsansvariges vägnar kallas för personuppgiftsbiträde i det här fallet. (Europesika Kommissionen, u.d.)

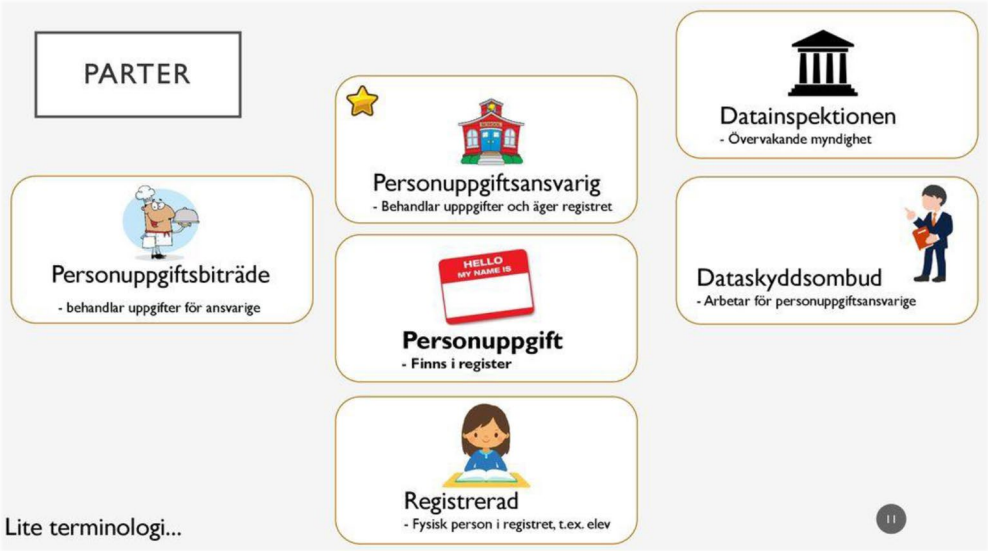
Skriftliga avtal krävs i två fall. När två eller fler är gemensamt ansvariga för en behandling som vi tidigare nämnde i texten eller när ett biträde anlitas som i det här fallet med lönehanteringsföretag. Personuppgiftsbiträdets plikter gentemot den personuppgiftsansvarige måste specificeras i ett avtal. Biträdesavtalet måste vara tillräckligt konkret vilket betyder att organisatoriska och tekniska säkerhetsåtgärder specificeras. Enligt GDPR i artikel 28.3 kommer det fram hur ett biträdesavtal behöver vara utformat (Europeiska unionens officiella tidning, 2016, s. art 28).

De flesta företag och organisationer som behandlar personuppgifter i en stor omfattning eller behandlar känsliga uppgifter kommer behöva utse ett dataskyddsombud (Europeiska unionens officiella tidning, 2016, s. art 37). Dataskyddsombud utses av personuppgiftsansvarige och personuppgiftsbiträdet om någon av nedanfrågor stämmer in i organisationen (Dataskyddsinspektionen, u.d.).

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

Dataskyddsombudets uppgifter är att informera och rådgiva personuppgiftsansvarige och personuppgiftsbiträdet samt kontrollera att dataskyddsförordningen (GDPR) inom organisationen följs. Ombudet ska även kontrollera att skyldigheterna följs enligt dataskyddslagstiftningen och ska vara datainspektionens kontaktperson (Europeiska unionens officiella tidning, 2016, s. art 39).

Figur 2 beskriver de viktiga roller inom GDPR:



Figur 2 - Parter vid behandling av personuppgifter (Slideplayer, 2018)

3 FORSKNINGSMETOD

I det här kapitlet presenteras valet av forskningsmetoden som vi har använt för att samla in data. Efter att metodvalet diskuterats kommer vi ta fram ett intervjuunderlag och presentera det baserat på teorin och forskningsfrågor. För att kunna besvara våra frågeställningar kommer vi genom intervjuer av våra respondenter på tre olika organisationer undersöka på en djupare nivå vilka konkreta åtgärder har de olika organisationer gjort samt vilka nya arbetsprocesser och rutiner har tagits i bruk.

3.1 Kvalitativ forskning

I detta arbete kommer vi att använda oss av en kvalitativ undersökningsmetod bestående av semistrukturerade intervjuer. Genom kvalitativa intervjuer kan vi förstå och förmedla intervjupersonernas upplevelser och perspektiv, medan i en kvantitativ studie är det snarare forskarens upplevelser och perspektiv som är till grund för hur undersökningen styrs (Bryman, 2002, s. 272).

Genom den kvalitativa datainsamlingen som vi valde i form av intervjuer kommer vi därför få en bättre förståelse för fallet vi undersöker. Det finns tre typer av intervjuformer som används strukturerade intervjuer, semistrukturerade intervjuer och ostrukturerade intervjuer. Vi ansåg att semistrukturerade intervjuer är mest lämpad för vårt examensarbete för att det tillåter oss en större frihet att gå in i en dialog med intervjupersonerna.

Bryman (2002) beskriver semistrukturerade intervjuer som ett bra alternativ. Man är inte lika mycket bunden till att ställa frågorna i just den ordningen som vi hade, utan det öppnar också upp möjligheten för oss att ställa följdfrågor (Bryman, 2002, s. 127).

Vi får också djupare förståelse från respondenterna om hur organisationer har anpassat sig till GDPR. Semistrukturerade intervjuerna kommer att utföras först efter att litteraturstudien är utförd. Det blir lättare för oss att ställa de rätta frågorna till respondenterna då vi har litteraturstudien klart. Två av intervjupersonerna föredrog att svara på frågorna utförligt via mejl. Ifall vi hade ytterligare frågor eller ville ha mera information så var dem villiga att hålla

intervju eller telefonsamtal om så behövs. Båda personerna gav oss möjligheten av tilläggsfrågor, vilket inte orsakade några problem för oss.

3.2 Intervjuernas genomförande

Intervjuerna genomfördes med hjälp av elva frågor som handlade om GDPR. Våra frågor ställdes i ordningsföljd, men det blev också en del följdfrågor för att öppna upp för diskussion. Som vi tidigare nämnde semistrukturerade intervjuer är mest lämpad för vårt arbete för att det tillåter oss en större frihet att gå in i en dialog med intervjupersonerna. Intervjupersonerna kommer från tre olika verksamheter och alla är aktivt involverade i verksamhetens arbete med GDPR. Enligt oss har de olika respondenterna tillräckligt med erfarenhet inom området för att kunna ge oss tillräcklig med information för att besvara våra frågeställningar. I vårt arbete kommer vi använda oss av personerna A och B, person C och person D. Personerna A och B arbetar i samma organisation.

Person C och person D föredrog att svara på frågorna utförligt via mejl. Intervju genomfördes via mail och möjligheten av tilläggsfrågor har också funnits, vilket var en fördel för oss. Personerna A och B som arbetar inom samma organisation valde vi att intervjua på dessa anställdas kontor. Innan vi började intervjua frågade vi intervjupersonerna om de ger tillåtelse för att intervjun spelas in för att säkerställa att all information från intervjuerna kommer med. En annan anledning till att vi spelade in intervjuerna var att fokusera bättre på själva intervjua och inte behöva skriva ner allt. Intervjun varade i ungefär 35 minuter.

3.3 Val av organisationer och presentation av dem

I det här kapitlet beskriver vi hur vi valde ut och kom i kontakt med organisationerna som deltagit i undersökningen. Vi presenterar kort val av verksamheterna och respondenterna som deltagit i undersökningen.

För de flesta organisationer och offentliga myndigheter på Åland leder GDPR till nya utmaningar. Vår målsättning under vår urvalsprocess var att hitta organisation eller myndighet som behandlar personuppgifter i sitt dagliga arbete.

Vissa gör det i större utsträckning och andra i mindre men alla påverkas av GDPR. För att nå ut till de företag vi tyckte var passande utgick vi från personliga kontakter på organisationer. De som var intressanta för oss valde vi att ta kontakt via telefon och mail. I mailet presenterade vi först oss och vårt examensarbete. Vi beskrev även syftet och frågeställningar och varför vi kontaktar dem. I mailet framkom också begreppet anonymitet där vi informerade att uppgifterna om organisationen och respondenterna kan behandlas anonymt om så önskas från deras sida. Som undersökningsobjekt valde vi ut en offentlig myndighet och två större verksamheter på Åland. Nedan följer en kort presentation vad som skiljer företagen eller myndigheten åt, och vad de erbjuder för tjänster.

Högskolan på Åland - är en myndighet under Ålands landskapsregering. Till verksamheten hör högskoleutbildning, öppna högskolekurser, fortbildningskurser och forskning.

Viking Line - är en åländsk rederikoncern med trafik på Östersjön. De erbjuder färjetransport, hamntjänster, passagerartransport, godstransporter, semester, affärsresor.

Ålands Ömsesidiga Försäkringsbolag - är ett skadeförsäkringsbolag som försäkrar bilar, hus, företag, djur och sedan 2019 även personer. Bolaget grundades redan 1866 och är förstås därmed ett av Ålands absolut äldsta företag. I folkmun kallas bolaget Ömsen, men heter egentligen Ålands Ömsesidiga Försäkringsbolag.

Det som vi letade efter hos alla företaget var att de erbjuder en viss form av tjänster, vilket betyder att de alla utför personuppgiftsbehandling. Organisationerna skiljer sig dock från varandra då det i varje organisation erbjuds skilda produkter och tjänster.

3.3.1 Val av relevanta intervjupersoner

Urvalet av intervjupersonerna valdes medvetet vilket betyder att vi siktade på intervjupersonerna som har en viss kunskap om GDPR. Intervjupersonerna kommer från tre olika verksamheter och alla är aktivt involverade i verksamhetens arbete med GDPR.

4 UNDERSÖKNINGENS INSAMLADE DATA

Intervjuerna gjordes enligt metoden i kapitel 3. Vi har fått olika svar från den olika intervjuobjekten, dem kommer vi benämna som personerna A och B som arbetar i samma organisation och personerna C och D som arbetar i de andra två organisationer. I det här kapitlet redogör vi för de svar vi fått av intervjupersonerna. Vi har valt att strukturera det på det viset att vi skriver ut frågorna som ställdes på intervjun och sedan skriver de olika intervjupersonernas svar på dem.

Har det skett konkreta ändringar i ert arbete pga. GDPR?

Personerna A och B som arbetar på Högskolan på Åland berättar att det var ganska mycket som har ändrats. Högskolan började skriva nya personuppgiftsbiträdesavtal som är ett krav av GDPR. Personerna nämner också att organisationen har upprättat en registerbeskrivning enligt GDPR som man kan finna på deras hemsidan. I registerbeskrivningen hittar man information om vilka uppgifter organisationen samlar in, varför de samlas och till vad det används. Personerna A och B berättar också att information om hantering av personuppgifterna finns också på deras hemsida. Där hittar man hur Högskolan på Åland hanterar studerandes personuppgifter. Alla registrerades rättigheter finns där nedskrivna.

Personerna nämner också hur de hanterar kameraövervakning. På deras hemsida finner man information om tydligt syfte med kameraövervakning och vilken typ av kameraövervakning organisationen använder samt på vilken rättslig grund. I och utanför fastigheten finns skyltning som informerar om kameraövervakning. I organisationen har de även infört låsta postfack där varje anställd har egen nyckeln till sitt låsta postfack. All utgående och ingående post är låst nu. En annan viktig sak som organisationen har gjort är rensning av onödiga uppgifter som inte längre behövs eller lagrats för länge. All personal har gått igenom vad dem har i egna arbetsrum, plockat bort allt som inte behövs längre.

Personen C berättar om att förberedelserna började redan i ett tidigt skede innan GDPR trädde i kraft och genom förberedelser deras verksamhet vidtog före GDPR trädde i kraft uppnådde de en mycket bättre kontroll över den data de har, såsom var den finns och hur den är skyddad, vilka har tillgång till den internt, och vilka externa partners de eventuellt delar

den med. Personen nämner också att internt har de blivit noggrannare med användarbehörigheter och hur de överför data med personuppgifter inom koncernen. Externt har de strävat till att informera kunder och övriga intressenter hur deras data behandlas. Verksamheten har till exempel inrättat en service där kunderna kan kontakta dem om de har frågor gällande behandlingen av sina personuppgifter, eller om de vill begära ut registerutdrag eller dylikt.

Personen D som är anställd i den tredje organisation säger att GDPR har orsakat en mängd åtgärder i bolaget. Som försäkringsbolag behöver de enligt regelverket ha ett dataskyddsombud, vilket de har tillsatt internt. Därtill har samtliga rutiner för personuppgiftshantering setts över och förbättringar har gjorts i många avseenden. Vidare säger personen att bolagets interna regelverk har utökats med bland annat en policy för personuppgiftshantering med flertalet underdokument. En process för personuppgiftsincidenter har infogats i riktlinjer för incidenthantering dessutom har bolaget utvecklat en systemkarta över samtliga system och en rutin för konsekvensanalys. Gällande lagring av personuppgifter genom molntjänster har bolaget intagit en restriktiv syn och avvaktar tydliggörande av rättsläget inom EU.

Vilket rättsligt stöd har ditt företag för behandling av personuppgifter? (samtycke, avtal, rättslig förpliktelse, myndighetsutövning)

Personerna A och B säger att de använder sig av flera rättsliga stöd men då det gäller studerande så används den lagliga myndighetsutövningen. Dessa rättsliga grunder är relevant för myndigheter och är vanliga inom högskolan. Vid fotografering kan de till exempel använda sig av samtycke.

Personen C berättar att deras organisation behandlar en stor mängd personuppgifter och för väldigt många olika syften där rättsliga grunder för behandlingen varierar enligt syfte. Organisationen har exempelvis en rättslig förpliktelse att registrera vissa uppgifter om passagerare som reser med deras fartyg, som kommer direkt från lagen om passagerarlistor på passagerarfartyg. För kunder som är medlemmar i deras lojalitetsprogram behandlar de uppgifter baserat på avtal. För anställdas del behandlas uppgifterna främst också baserat på arbetsavtalsförhållandet. Verksamheten kan också i vissa fall behandla personuppgifter baserat på intresseavvägning.

Personen D säger att behandlingen av personuppgifter baserar sig på avtal (försäkringsavtal). Under den här frågan ställde vi också en extra fråga endast till försäkringsbolaget som gäller behandlingen av känsliga personuppgifter.

För att kunna behandla känsliga personuppgifter räcker det inte att finna en rättslig grund i artikel 6 utan ett undantag i artikel 9.2 måste också vara tillämpligt. Om företaget behandlar känsliga personuppgifter måste det finnas övertygande skäl till registreringen och man måste kunna visa detta. Dessutom måste känsliga personuppgifter ha ett extra bra skydd så att inga obehöriga kan komma åt dem.

Hur gör ni här, då det är frågan om exempel hälsouppgifter?

Personen D säger att i vissa avseenden är hanteringen av ärenden hos dem att anse som myndighetsutövning – detta kan gälla de lagstadgade försäkringar som försäkringsbolaget erbjuder, innefattande trafikförsäkring och lagstadgat arbetsolycksfall. Inom ramen för dessa försäkringar kan hantering av hälsouppgifter vara nödvändiga för att kunna tillvarata de intressen som försäkringarna avser skydda. Därtill kan behandling av känsliga uppgifter vara aktuella inom vissa frivilliga försäkringar. Behandling av sådana uppgifter sker inom ramen för dessa försäkringar enbart när det är nödvändigt för att tillvarata försäkrade intressen. Vidare berättar personen att tillgången till känsliga personuppgifter är begränsad till de anställda som måste komma åt uppgifterna för att kunna utföra sina arbetsuppgifter. Förutom genom behörighetsbegränsningar i bolagets interna system, skyddas uppgifterna på flera andra sätt. Anställda i bolaget undertecknar sekretessförbindelser och sekretess iakttas även mellan olika avdelningar inom bolaget, aktivitet i bolagets interna system loggas, m.fl. skyddande åtgärder.

Har GDPR medfört fördelar till ert arbete?

Personerna A och B berättar att stora fördelen med GDPR är säkerheten. Personerna betonar vikten i att kunden kan känna sig säker med hur saker och ting sköts. Som fördelar för Högskolan listar personerna A och B bland annat att de har full koll på vad samlas in för uppgifter men även var alla uppgifter finns.

Personen C berättar att de har en bättre kontroll över deras data samt skyddet har ökat. Person C nämner att i nuläge är det inte så arbetsamt pga. GDPR, det var närmast under omställningen inför att GDPR började tillämpas som arbetsbördan var som störst.

Vidare berättar personen att GDPR har blivit en realitet för alla deras samarbetspartners eller avtalspartners. Det finns en mycket bättre förståelse varför vissa saker måste skötas på ett visst sätt. Detta gör att avtalsförhandlingar nu är mycket smidigare och att leverantörers produkter är färdigt GDPR-anpassade.

Personen D berättar att regelverksförändringar är ofta ett bra tillfälle att utvärdera och förbättra sina interna processer, vilket de också gjort med anledning av GDPR. Det interna regelverket har utökats med fler och mer utförliga specifika beskrivningar av olika dataskyddsrelaterade frågor, vilket tydliggör hanteringen. Därtill införs genom anpassningarna till regelverket många funktioner i system och andra förbättringar som de kanske önskat en längre tid, men som bolaget i samband med GDPR nu verkligen har tillsett att frigöra resurser för. Systemen ses över på ett mer ingående och noggrant sätt, behörighetsbegränsningarna har utökats, loggningen av system har förbättrats och många processer har förtydligats.

Har GDPR medfört nackdelar till ert arbete?

Personerna A och B säger att det har varit tidskrävande, men de ser det inte som nackdel. Uppskattningsvis har det gått tusentals timmar till allt.

Personen C berättar att själva omställningsprocessen var krävande och arbetsdryg. Förutom det har det knappast medfört några större nackdelar som markant påverkar vardagen.

Som nackdelar listar person D främst de extra kostnader som har uppstått genom merarbete både i utrednings- och utvecklingsfasen inför ikraftträdandet av GDPR men även kontinuerligt kräver det mer tid av interna resurser i och med att det kontinuerligt sysselsätter dataskyddsombud, bolagets jurister samt IT-personal. Vidare nämner personen att därtill berörs även övrig personal i bolaget genom att de utbildas och fortbildas varje år samt genom att det tillkommit vissa nya frågor att beröra i den dagliga verksamheten samt i bolagets olika utvecklingsprojekt.

Personen D ser inget negativt med utbildning och fortbildning utan är tvärtom ett välkommet inslag – men som nackdel sett så kräver det viss tid. Vidare säger personen att nya projekt kräver mer tid och resurser än tidigare med nya frågeställningar att beakta samt extra arbetsmoment. Det ställs idag stora krav, rent regelefterlevnadsmässigt, när någon typ av ny insamling av personuppgifter skall utföras eller när något i behandlingen ändrar – t.ex. behörighetsmässigt, säkerhetsmässigt eller annat.

Har sättet som ni lagrar information på ändrat?

Personerna A och B berättar att själva sättet har inte ändrats utan tillgången till det, organisationen använder fortfarande samma system. Vidare säger personerna att Google molntjänster togs i bruk före GDPR blev aktuellt. Google molntjänster är en fördel på visa sätt men också begränsade på de sättet att man inte sätter ut på den vad som helst.

Personen C säger att organisationen har förbättrat det infrastrukturella skyddet för deras personuppgifter och ökat behörighetsstyrning inom koncernen (dvs vilka medarbetare har tillgång till vilken information).

Person D berättar att riktlinjerna för lagring av information är striktare än tidigare och deras interna system har utvecklats för att vara mer ändamålsenliga. Vidare berättar personen att sparad information kategoriseras i större utsträckning än tidigare för att underlätta sökning och annan hantering. Lagringstiderna för olika typer av information har setts över och dokumenterats. Anpassningar för automatisering av radering av uppgifter som uppnår maximal lagringstid har gjorts.

Har sättet som ni kommunicerar med era kunder på förändrats?

Personerna A och B säger att Högskolan informerar på studerandeportalen hur de hanterar studerandes personuppgifter. Information om kameraövervakning finns skyltning nu utanför fastigheten. Känsliga personuppgifter som behöver kommuniceras sköts exempelvis genom studerandes e-post ha.ax som är internt skyddat.

Personen C säger det har inte ändrat så markant. Organisationen har sett till att de inte lagrar sådana personuppgifter som de inte är skyldiga att lagra/behöver lagra/skall lagra. När dem inte har dessa uppgifter så behöver dem inte vara rädda för att kommunicera. Vidare säger personen C när det handlar om känsliga personuppgifter som behöver kommuniceras sköts detta exempelvis genom kryptera e-post eller andra kanaler.

Personen D säger kommunikation som innehåller personuppgifter alltid har behövt ske med försiktighet, även innan GDPR. Men riktlinjerna kring hanteringen har utökats och förtydligats. Kommunikation via e-post skall ske via säker linje/krypterat.

Har personalen utbildats? På vilket sätt?

Personerna A och B säger att alla erbjöds utbildning som har gått både extern och intern. Kameradirektivet kom föra året och i år kom informationshanteringslagen och det krävs kontinuerlig utbildning.

Personen C berättar att hela koncernen har genomgått en allmän elektronisk GDPR-skolning under tidiga 2018. De har också kört så kallade refresher-kurser åt i synnerhet personalavdelningarna och IT.

Personen D säger att dataskyddsombud, IT-personal och jurister har gått externa utbildningar. Samtliga anställda hos Ömsen går även kontinuerligt utbildning inom dataskydd, som både hålls av bolagets jurister men även genom ett utbildningsprogram levererat av extern tjänsteleverantör.

Hur har era kunder reagerat?

Personerna A och B berättar att de inte har hört något negativt i samband med förändringen. Vissa studerande är mer uppdaterade och visa har inte så stora tankar kring det.

Personen C säger i det stora hela har kunderna inte reagerat väldigt starkt. Vissa kunder är måna om sina rättigheter och önskar bli bortglömda. Vissa begär registerutdrag för att använda dem som underlag till beskattning eller försäkringsärenden. De flesta kontakter de får i detta sammanhang är från kunder som vill avregistrera sig från marknadsföring.

Personen D säger att de inte har märkt något särskilt hos deras kunder, dem har inte heller fått några särskilda GDPR-relaterade frågor.

Har GDPR medfört mycket kostnader?

Personerna A och B säger att det har uppstått visa kostnader för plattformar, men det mesta är personliga resurser.

Personen C berättar att en del kostnader har naturligtvis förekommit i och med omställningen, men de jobbar i en bransch som är väldigt strikt reglerad och nya myndighetskrav är vardag. De arbeten GDPR har medfört har således inte stått ut kostnadsmässigt.

Personen D säger att översynen av regelefterlevnaden av GDPR och dess implementering i verksamheten har kostat i utredningskostnad genom visst bistånd av konsult innan dataförordningens ikraftträdande. Efter det har de dock uteslutande hanterat övriga GDPR-relaterade frågor och utredningar internt inom bolaget, vilket förstås också är att betrakta som en kostnad. Ett dataskyddsombud har rekryterats internt och en intern projektgrupp för GDPR-frågor har tillsatts, som sammanträder kontinuerligt.

Vidare säger personen att dataskyddsombud, IT-personal och jurister har gått externa utbildningar. Samtliga anställda hos Ömsen går även kontinuerligt utbildning inom dataskydd, som både hålls av bolagets jurister men även genom ett utbildningsprogram levererat av extern tjänsteleverantör. Utbildningen innebär således också en viss kostnad både i tid för samtliga i personalen, men även i direkt kostnad genom programinköp samt fortbildning av dataskyddsombud och övriga anställda som dagligen är involverade i dataskyddsfrågor.

5 RESULTAT OCH ANALYS

I det här kapitlet presenteras empirin från våra intervjuer och analyseras med teorin som grund. Resultatet kommer bygga på de frågorna som tidigare presenterats, dvs. vilka konkreta åtgärder har de åländska verksamheterna gjort och vilka nya arbetsprocesser och rutiner har tagits i bruk. Vi kommer att ta upp respondenternas svar och koppla dem till litteratur och tidigare forskning. Citaten i detta kapitel är utdrag från intervjuerna, där de fullständiga intervjuerna kan hittas. Att använda sig av både teori och forsknings delen bidra ett djupare kunskap om resultatet samtidigt får man en bättre bild på vad som är likställt eller skiljer sig åt i litteraturen och i respondenternas svar. Våra två frågor som vi ställde i frågeställningen kommer vi besvara genom rubrik 4 där vi har samlat in data från våra intervjuer som sedan kompletteras med teorin vi hade skrivit.

Hur har de tre organisationerna på Åland påverkats av GDPR? Vilka konkreta åtgärder har de vidtagit samt vad har de gjort för att anpassa sig?

EU:s allmänna dataskyddsförordning (GDPR) tillämpades den 25 maj 2018, efter en två års övergångsperiod. Det betyder att alla företag, myndigheter, föreningar etc. som behandlar personuppgifter har haft en lång tid att anpassa sig till det nya regelverket, samt påvisa att deras verksamhet följer nya reglerna i EU:s allmänna dataskyddsförordning.
GDPR berör alla organisationer och verksamheter på Åland som på något sätt samlar in och hanterar personuppgifter. För organisationer och verksamheter på Åland innebär det att de måste se till att deras arbetsrutiner inte på något sätt går mot GDPR och att de måste kunna påvisa att deras verksamhet följer nya regelverket.

Datainspektionen har en checklista för personuppgiftsansvariga om förberedelse innan GDPR trädde i kraft. Utdrag från intervjuerna hur alla tre organisationer var förberedda inför dataskyddsförordningen börjar på nästa sida (Samlogic Software Blogg, 2018).

”Personen B berättade att Högskolan på Åland har sedan tidigare följt den svenska Personuppgiftslagen, PUL. Så arbetet med integritet har nog funnits tidigare men tack vare GDPR så blev det "lättare" att vrida åt vissa "kranar" t.ex. genom att hänvisa till behörighet endast vid konkreta behov och "bra att ha" filosofin kunde skrotas.”

”Vidare berättade personen B att datasäkerhetspolicy och säkerhetstänk inom samma kategorier som idag har nog funnits över tio år här men naturligtvis eskalerat på grund av (tack vare) en mera global och digital värld.”

”Personen C tagit upp att deras verksamhet har arbetat med förordningen före GDPR trädde i kraft. Genom förberedelserna som de vidtagit före GDPR trädde i kraft uppnådde deras organisation en mycket bättre kontroll över den data de har, såsom var den finns och hur den är skyddad, vilka har tillgång till den internt, och vilka externa partners de eventuellt delar den med.”

”Personen D berättade att inför GDPR:s ikraftträdande vidtogs en rad åtgärder för att kunna genomföra eventuella förändringar och förbättringar som behövdes. Inom bolaget tillsattes en projektgrupp som arbetade kontinuerligt med dessa frågor, tillsammans med en stödfunktion som var externt tillsatt. Genom arbetet som gjordes och åtgärderna som vidtogs uppnåddes bland annat en bättre kontroll över bolagets data, konsekvensanalys av system, tydligare interna regelverk, uppdaterade avtal angående datasäkerhet med såväl anställda som externa parter samt utökad utbildning av personalen inom dataskydd. Den interna gruppen arbetar därtill vidare med utvärdering och ytterligare förbättringar av redan vidtagna åtgärder.”

När vi kommer till förberedelser inför dataskyddsförordningen så har alla respondenterna svarat att deras organisation var på något sätt redan förberedda innan GDPR trädde i kraft. Organisationerna har redan bildat sig en uppfattning om den nya regleringen innan den kom samt var väl medvetna om den nya lagen.

Personen D berättade att inom deras bolag så tillsattes en projektgrupp som arbetade kontinuerligt med dessa frågor, tillsammans med en stödfunktion som var externt tillsatt vilket betyder att dem var väl insatta i GDPR och uppfyllde redan flera punkter av datainspektionens checklista. Här kan vi se en sammankoppling mellan teorin och intervjupersonens svar att de redan har säkerställt vilka i bolaget som bär de olika roller och vad deras ansvar är samt att de kontinuerligt arbetar med sina ansvarsområden.

Kapitel 2.2 tar upp de grundläggande principer för behandling av personuppgifter. Där nämndes också hur viktigt det är att endast de som behöver någon specifik lagrad information har tillgång till den. All information som organisationerna har lagrat och innehåller personuppgifter ska alltså inte vara tillgänglig för alla anställda om inte alla behöver den.

”Personerna A och B berättade i deras intervju att i organisationen har de infört låsta postfack där varje anställd har egen nyckeln till sitt låsta postfack. All utgående och ingående post är låst.”

”Personen C berättade att de har blivit internt noggrannare med användarbehörigheter och hur dem överför data med personuppgifter inom koncernen. Externt har de strävat till att informera kunder och övriga intressenter hur deras data behandlas.”

”Personen D berättade att tillgången till känsliga personuppgifter är begränsad till de anställda som måste komma åt uppgifterna för att kunna utföra sina arbetsuppgifter. Förutom genom behörighetsbegränsningar i bolagets interna system, skyddas uppgifterna på flera andra sätt. Anställda i bolaget undertecknar sekretessförbindelser och sekretess iakttas även mellan olika avdelningar inom bolaget, aktivitet i bolagets interna system loggas, m.fl. skyddande åtgärder.”

Här hittas en klar sammankoppling mellan teori och intervjupersonernas svar. Det kom fram att alla tre organisationerna uppfyller punkterna om tillgång till lagrad information.
När vi kommer till lagring av personuppgifter så gäller följande för organisationer: de måste informera den registrerade varför de lagrar uppgifterna, vidare måste de också informera personen hur länge det är tänkt att personuppgifterna ska lagras. I kapitel 2.2 nämns det att personuppgifterna inte skall sparas under längre tid än vad som är nödvändigt för ändamålet. De personuppgifter som inte längre behövs ska raderas eller avidentifieras efter en viss tid.

Under rubriken 2.2 framkommer också en punkt om ändamålsbegränsning. Detta innebär när ett företag eller organisation samlar in personuppgifter måste de vara säkra vad de ska användas till från början och förmedla det till den registrerade. Ändamålet skall vara tydlig innan personuppgifterna samlas in.

Insamling av personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Organisationerna ska kunna visa att det följer dessa principer.

”Personerna A och B berättade under intervjun att deras organisation har gjort rensning av onödiga uppgifter som inte längre behövs eller lagrats för länge. All personal har gått igenom vad de har i egna arbetsrum, plockat bort allt som inte behövs längre. Personerna nämner också att organisationen har upprättat en registerbeskrivning enligt GDPR som man kan finna på deras hemsidan. I registerbeskrivningen hittar man information om vilka uppgifter organisationen samlar in, varför de samlas och till vad det används.”

”Personen C berättat att dem har sett till att de inte lagrar sådana personuppgifter som de inte är skyldiga att lagra, behöver lagra eller skall lagra. När de inte har dessa uppgifter så behöver de inte vara rädda för att kommunicera. Personen C nämnde också att de har till exempel inrättat en service där kunderna kan kontakta dem om de har frågor gällande behandlingen av sina personuppgifter, eller om de vill begära ut registerutdrag eller dylikt. De har infört automatiserade gallringsrutiner för personuppgifter i deras kundsystem, där uppgifterna anonymiseras eller raderas efter en viss tid.”

”Personen D berättade under intervju att riktlinjerna för lagring av information är striktare än tidigare och deras interna system har utvecklats för att vara mer ändamålsenliga. Sparad information kategoriseras i större utsträckning än tidigare för att underlätta sökning och annan hantering. Lagringstiderna för olika typer av information har setts över och dokumenterats. Anpassningar för automatisering av radering av uppgifter som uppnår maximal lagringstid har gjorts.”

I alla tre intervjuerna kommer det klart fram att det har skett ett omfattande arbete när det gäller lagring av personuppgifterna och till vilket ändamål dem används. Insamling av personuppgifter samlas endast in för särskilda, uttryckligt angivna och berättigade ändamål och onödiga plockas bort. Det vi kan konstatera är att de registrerade kan vara säkra hur deras personuppgifter behandlas, då man ser på hur tre stora organisationer på Åland nuförtiden gör sitt arbete.

I kapitel 2.3 har vi skrivit om de rättsliga grunderna för behandling av personuppgifterna. Detta innebär att behandling av personuppgifter får endast ske under de omständigheter som

lyfts fram i lagstiftningen. För att en personuppgiftsbehandling ska vara laglig måste de sex olika rättsliga grunder som anges i det officiella GDPR-dokumentet följas.

”Personerna A och B berättade att deras myndighet använder lagliga myndighetsutövningen. Vid fotografering kan de exemplen använda sig av samtycke också.”

”Personen C berättade att deras organisation behandlar en stor mängd personuppgifter och för väldigt många olika syften, rättsliga grunder för behandlingen varierar enligt syfte. Exempel på några är avtal, intresseavvägning samt en rättslig förpliktelse som kommer direkt från lagen om passagerarlistor på passagerarfartyg.”

”Personen D berättade att behandlingen av personuppgifter baserar sig på avtal (försäkringsavtal).” Här ställdes också en extra fråga endast till försäkringsbolaget som gäller behandlingen av känsliga personuppgifter.

”Personen D berättat att de kan använda myndighetsutövning när de kommer till de lagstadgade försäkringar som försäkringsbolaget erbjuder, innefattande trafikförsäkring och lagstadgat arbetsolycksfall. Inom ramen för dessa försäkringar kan hantering av hälsouppgifter vara nödvändiga för att kunna tillvarata de intressen som försäkringarna avser skydda. Därtill kan behandling av känsliga uppgifter vara aktuella inom vissa frivilliga försäkringar.”

Datainspektionen skriver att den delen av personalen i en organisation som behandlar personuppgifter eller känsliga personuppgifter måste utbildas i sina arbetsrutiner. Det kommer klart fram av intervjupersonen D att man inom deras organisation har satsat på utbildning och att samtliga anställda hos Ömsen går även kontinuerligt utbildning inom dataskydd, som både hålls av bolagets jurister men även genom ett utbildningsprogram levererat av extern tjänsteleverantör.

Personuppgiftsbehandlingen är laglig om en rättslig grund finns bakom behandlingen. Det kommer klart fram av alla fyra intervjupersonerna att de använder sig av rättsliga grunder vid behandling av personuppgifterna. Exempel om vilken rättslig grund utgår de olika organisationer på Åland ifrån när de behandlar registrerandes personuppgifter finner vi i ovannämnda utdrag från intervjuerna.

Datainspektionen skriver om nya rutiner för behandling av personuppgifter. Detta innebär att organisationerna i samband med GDPR måste se till att deras arbetsrutiner inte på något sätt går mot GDPR. De tre organisationerna ska kunna bevisa att lämpliga tekniska och organisatoriska åtgärder har genomförts (Datainspektionen, u.d.).

''Personerna A och B listade några nya rutiner som kom i samband med GDPR. De har en GDPR-policy som revideras och ses över vid behov. Teckning av nya biträdesavtal med samarbetspartners har tillkommit. De upprättar registerbeskrivningar samt jobbar kontinuerligt med att förbättra datasäkerheten."

"Personen C berättade att de har tagit i bruk en tjänst där kunder kan begära ut ett registerutdrag över sina uppgifter. I tjänsten undertecknar med stärkt autentisering (bankkoder) ett specifikt formulär. På det sättet kan vi vara säkra om att rätt uppgifter skickas till rätt person. Vi har också tagit i bruk en tjänst för kryptering av email, så att vi kan skicka personuppgifter ut ur bolaget på ett säkert sätt. Organisationen gör också personuppgiftsbiträdesavtal när dem anlitar nya personuppgiftsbiträden."

"Personen D nämnde att genom GDPR har flera nya arbetsmoment tillkommit, såsom exempelvis personuppgiftsbiträdesavtal och konsekvensanalyser av system m.m."

Om vi utgår från intervjuerna vad de olika respondenterna har sagt om deras nya arbetsrutiner som har tagits i bruk i samband med GDPR, kan vi konstatera att alla tre organisationer har sett över sina arbetsrutiner och att de har blivit mycket säkrare för den registrerade. Ett exempel på det är att alla fyra respondenterna nämnde att nya personuppgiftsbiträdesavtal har tillkommit. I kapitel 4 kan vi läsa mera om personuppgiftsbiträdesavtal. Man har även i alla tre verksamheter kunnat konstatera att hela den interna säkerheten har uppnått en högre nivå i samband med det nya regelverket.

Personerna A och B nämnde också hur införandet av GDPR har lett till en förbättring av säkerheten som helhet.

6 DISSKUSION OCH SLUTSATS

I det här kapitlet sker studiens slutsats och diskussion som kommer att presenteras genom respondenternas åsikter och koppla dem till litteratur och tidigare forskning. I slutet kommer vi att nämna vad vi tycker skulle vara intressant att utforska vidare. Vi kommer att presentera och diskutera det resultat vi har fått. I vår undersökning har vi avgränsat oss till att undersöka endast de större organisationer på marknaden, men det är fullt möjligt att GDPR skulle se annorlunda ut i mindre företag.

Det officiella GDPR-dokumentet är mycket omfattande. Det är ett detaljerat arbete på 119 sidor med 99 artiklar och 173 skäl, vilket lämnar en del att tolka. GDPR är en noggrant och detaljerad lagstiftning, men den måste ändå analyseras omsorgsfullt.

För att förbereda sig inför de stora förändringar som GDPR innebär är det viktigt att i tid sätta sig in de nya regleringarna, vilket våra respondenter har också gjort. Deras organisation har redan bildat sig en uppfattning om den nya regleringen innan den kom samt var väl medvetna om den nya lagen. Huvudsyftet med intervjuerna var att ta reda på hur och vad organisationerna på Åland konkret har gjort för att följa förordningen, som togs i bruk den 25 maj 2018.

I resultat och analysen lyfts det fram de sammankopplingar som finns mellan teorin och den kvalitativa undersökningen. Vi har hittat tydliga sammankopplingar och kan se att alla tre organisationer påpekar att den stora delen av anpassningen till GDPR är organisatoriska förändringar såsom nya arbetsprocesser och utbildning av personal för att hantera det på ett säkert och lagligt sätt.

Det viktigaste med förordningen är att alla i organisationen känner till vilka data deras system lagrar och varför. Organisationerna skall kunna svara på varför de behöver uppgifterna, hur samlas de in och vem har tillgång till dem.

I kapitel 5 resultat och analys lyfts fram hur viktigt det är att endast de som behöver någon specifik lagrad information har tillgång till den.

Utifrån de vi har intervjuat kan vi säga de har kunnat besvara vilka typer av personuppgifter de hanterar, hur dem samlas in samt till vilket ändamål. Dem har även utökat informationskrav till den registrerade. En annan gemensam del är att organisationerna sett över sina arbetsrutiner, så att personer endast har tillgång till den information som de faktiskt behöver och att tillgången till lagrad information är begränsad enligt det nya lagkravet.

I kapitel 2.2 finner vi en viktig rubrik ”De grundläggande principerna” som gäller för all behandling av information. Principerna ses vara kärnan i förordningen och det är viktigt att organisationerna förstår och tillämpar dem. Här har vi hittat tydliga sammankopplingar mellan teorin och den kvalitativa undersökningen. Det kom fram av alla respondenterna som vi intervjuat, att deras organisation följer grundläggande principer för behandling av personuppgifter och att behandlingen endast utförs på laglig grund. De lagliga grunderna nämns i kapitel 2.3. Även här svarade alla respondenter att det finns ett rättslig grund bakom deras behandlingar.

Enligt dataskyddsförordningen räcker det inte att organisationerna bara följer de skyldigheterna som framkommer i GDPR-lagen utan det skall även framkomma hur skyldigheterna ska uppfyllas vilket betyder att organisationerna skall genomföra lämpliga åtgärder för att säkerställa att behandlingen sker i enlighet med förordningen, vilket de tre verksamheterna som vi intervjuat har gjort också gjort. De största ändringarna som alla tre organisationer har gjort är kommunikation och informationsutbyte med kunden.

Enligt vår undersökning går det att generalisera resultatet att organisationerna har vidtagit nya tekniska och organisatoriska säkerhetsåtgärder för att deras kunder skall känna sig trygga med att deras insamlade personuppgifter ska behandlas säkert och enligt lagen. En av våra respondenter svarade att de infört automatiserade gallringsrutiner för personuppgifter i deras kundsystem, där uppgifterna anonymiseras eller raderas efter en viss tid.

Organisationerna har även säkerställt vilka i företagen som bär de olika roller och vad deras ansvar innebär samt se till att de kontinuerligt arbetar med sina ansvarsområden.

Efter vår analys av intervjuerna tycker vi att respondenternas svar har gett oss en bra bild på de konkreta åtgärder som deras organisationer gjort för att anpassa sig till den nya dataskyddsförordningen. Vi tycker att vi fått utförliga svar från de vi intervjuat. Vi bedömer att det inom de organisationer vi intervjuat hos fanns tillräckligt många konkreta förändringar och att dem har kunnat påvisa att deras verksamhet följer nya regelverket.

Vi tycker att det är viktigt att GDPR efterlevs. Organisationerna skall arbeta aktivt att möta kraven enligt nya dataskyddsförordningen samt kontinuerligt informera och utbilda medarbetare om GDPR och säkerhet. De skall se till att det sker ständigt utveckling och säkerställning av IT-miljön och tillhörande utrustning. Ett bra exempel på det som en av våra respondenter berättade är när deras organisation är på väg att ta i bruk ett nytt system kontrolleras alltid att det efterlever GDPR och att de i och med det nya systemet fortsättningsvis bibehåller deras kontroll över data.

Det finns ett par saker som vi tyckte kan vara intressant att undersöka vidare. Exempel genom att undersöka hur de mindre företagen på Åland med mindre resurser har anpassat sig till den nya dataskyddsförordningen. Dessutom kunde man undersöka kundernas rättigheter som GDPR har medfört.

KÄLL- OCH LITTERATURFÖRTECKNING

Ålands lagting. (den 13 12 2018). Hämtat från Lagförslag från Ålands landskapsregering LF 9/2018-2019: https://www.lagtinget.ax/arenden/LF%209%7C2018-2019/lagforslag-fran-alands-landskapsregering-lf-9-2018-2019-48964

Ålands landskapsregering. (den 29 08 2019). Hämtat från Landskapslag (2019:9) om dataskydd inom landskaps- och kommunalförvaltningen: https://www.regeringen.ax/alandsk-lagstiftning/alex/20199

Ålands Landskapsregering. (den 29 08 2019). Hämtat från https://www.regeringen.ax/alandsk-lagstiftning/foraldrad-lagstiftning/200788

Äldrecentrum. (den 24 09 2018). Hämtat från Dataskyddsförordningen: https://www.aldrecentrum.se/om-%C3%A4ldrecentrum/dataskyddsf%C3%B6rordningen-gdpr

Bryman, A. (2002). *Samhällsvetenskapliga metoder.* Trelleborg: Liber Ekonomi.

Datainspektion. (u.d.). Hämtat från Sanktionsavgifter och varningar: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/sanktionsavgifter-och-varningar/

Datainspektionen. (u.d.). Hämtat från Dataskyddsförordningens syfte och tillämpningsområde: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-syfte-och-tillampningsomrade/

Datainspektionen. (u.d.). Hämtat från Det här behöver ni veta: https://www.datainspektionen.se/vagledningar/for-foreningar-och-sma-organisationer/det-har-behover-ni-veta/

Datainspektionen. (u.d.). Hämtat från Samtycke: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/samtycke/ den 04 03 2020

Datainspektionen. (u.d.). Hämtat från Avtal med den registrerade: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/avtal-med-den-registrerade/ den 07 03 2020

Datainspektionen. (u.d.). Hämtat från Intresseavvägning: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/intresseavvagning/ den 07 03 2020

Datainspektionen. (u.d.). Hämtat från Rättslig förpliktelse: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/rattslig-forpliktelse/ den 07 03 2020

Datainspektionen. (u.d.). Hämtat från Ansvarsskyldighet: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/#Ansvarsskyldighet den 27 4 2020

Datainspektionen Åland. (2018). Hämtat från DI.AX: https://www.di.ax/

Dataskyddsinspektionen. (u.d.). Hämtat från Dataskyddsombud: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsombud/maste-vi-utse-ett-dataskyddsombud/ den 27 4 2020

Dataskydsinspektionen. (u.d.). Hämtat från Skydda grundläggande intressen: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/skydda-grundlaggande-intressen/

Di.ax. (u.d.). Hämtat från Principer för behandling av personuppgifter: https://www.di.ax/rattigheter-och-skyldigheter/principer-behandling-personuppgifter

Eduskunta riksdagen. (den 01 03 2018). Hämtat från Regeringens proposition: https://www.eduskunta.fi/SV/vaski/HallituksenEsitys/Sidor/RP_9+2018.aspx

Europeiska Kommisionen. (u.d.). Hämtat från När är ett samtycke giltigt: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_sv den 20 4 2020

Europeiska kommissionen. (u.d.). Hämtat från EU-lagstiftningen: https://ec.europa.eu/info/law/law-making-process/applying-eu-law_sv

Europeiska unionens officiella tidning. (den 4 5 2016). Hämtat från Europesika Kommissionen: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=sv

Europeiska unionens officiella tidning. (den 4 5 2016). Hämtat från Europesika Kommissionen: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=sv

Europeiska unionens officiella tidning. (den 4 5 2016). Hämtat från Europeiska Kommissionen: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=sv

Europeiska unionens officiella tidning. (den 05 04 2016). *Europaparlamentets och rådets förordning 2016/679*, s. 1. Hämtat från https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=sv

Europesika Kommissionen. (u.d.). Hämtat från Vad är en personuppgiftsansvarig eller ett personuppgiftsbiträde: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_sv den 20 4 2020

Fridlinger, D. (2018). *GDPR - juridik, organisation och säkerhet enligt dataskyddsförordningen.* Stockholm: Nortsteds Jurdik.

GDPR Grunder: Skillnad. (den 28 2 2018). Hämtat från DP Orginizer: https://www.dporganizer.com/sv/skillnad-personuppgiftsbitrade-personuppgiftsansvarig/

Högskolan i Borås. (den 18 12 2019). Hämtat från Myndighetsutövning och allmänt intresse: https://www.hb.se/Anstalld/For-mitt-arbete/Informationshantering/Behandling-av-personuppgifter-GDPR/Allman-information/Grundlaggande-principer/Rattslig-grund/Myndighetsutovning--allmant-intresse/

Multisoft. (u.d.). Hämtat från www.multisoft.se/gdpr/vad-betyder-pseudonymisering/: https://www.multisoft.se/gdpr/vad-betyder-pseudonymisering/

Samlogic. (u.d.). Hämtat från https://www.samlogic.com/articles/gdpr-eu-dataskyddsforordningen-foretag-organisationer.htm

Samlogic Software Blogg. (den 8 5 2018). Hämtat från https://www.samlogic.com/blogg/2018/05/datainspektionens-checklista-for-personuppgiftsansvariga-och-gdpr-guiden/

Slideplayer. (2018). Hämtat från Personuppgifter i skolan: https://slideplayer.se/slide/14878196/ den 12 05 2020

Wetterberg, M. W. (2019). *GDPR-Förstå och tillämpa i praktiken.* Stockholm: Sanoma Utbildning AB.

BILAGOR

Bilaga 1. Intervjufrågor

1) Vad har du/ni för roll inom företaget?

2) Vilka ändringar har det skett i ert arbete pga. GDPR? Några konkreta åtgärder som ni har vidtagit?

3) Vilket rättsligt stöd har ditt företag för behandling av personuppgifter? (Samtycke, avtal, rättslig förpliktelse Ett exempel: bokföringsskyldigheten, intresseavvägning)

   3.1) För att kunna behandla känsliga personuppgifter räcker det inte att finna en rättslig grund i artikel 6 utan ett undantag i artikel 9.2 måste också vara tillämpligt. Om företaget behandlar känsliga personuppgifter måste det finnas övertygande skäl till registreringen och man måste kunna visa detta. Dessutom måste känsliga personuppgifter ha ett extra bra skydd så att inga obehöriga kan komma åt dem.

   Hur gör ni här, då det är frågan om exempel hälsouppgifter?

4) Har GDPR medfört fördelar till ert arbete? Exempel på nedanstående?

5) Har GDPR medfört nackdelar till ert arbete? (tidskrävande, extra kostnader?)

6) Har sättet som ni lagrar information på ändrat?

7) Har sättet som ni kommunicerar med era kunder på förändrats? (Exempel: e-posten inte alls används för att dela information som innehåller personuppgifter)

8) Har personalen utbildats? På vilket sätt?

9) Hur har era kunder reagerat?

10) Har GDPR medfört mycket kostnader? (exempelvis förnya avtalen och skriva om bilagorna, inskolningen av personalen, implementeringen av de nya plattformarna)

Följdfrågor som ställdes i efterhand

11) Har er organisation/ myndighet haft några förberedelser innan GDPR trädde i kraft?