YRKESHÖGSKOLAN
NOVIA

GDPR i praktiken

Dataskyddsförordningens påverkan på ämbetsverk

Jennifer Lindholm

Examensarbete för företagsekonomi (YH)-examen

Tradenom

Vasa 2022

EXAMENSARBETE

Författare: Jennifer Lindholm

Utbildning och ort: Tradenom, Vasa

Inriktning: Justitieförvaltning

Handledare: Mayvor Höglund

Titel: GDPR i praktiken – Dataskyddsförordningens påverkan på ämbetsverk

---

Datum: 18.11.2022 Sidantal: 35 Bilagor: 1

Abstrakt

På grund av digitaliseringen och dess snabba utveckling infördes en dataskyddsförordning.

Förordningen togs i bruk i maj 2018. Dataskyddsförordningen tog i bruk för att öka säkerheten av behandling av personuppgifter och säkerställa trygghet för fysiska personer gällande deras personuppgifter och rättigheter som kommer till det.

Ämbetsverk behandlar personuppgifter på en daglig basis och en del av personuppgifterna kan vara känsliga för personer och därför är det viktigt att förordningens principer följs till punkt och pricka. Om inte ämbetsverk följer förordningen kan ämbetsverk få en administrativ sanktionsavgift att betala.

Syftet med detta arbete är att ta reda på hur ämbetsverk behandlar personuppgifter, hur personuppgifterna samlas in och vart de hamnar samt vad det finns för risker och riktlinjer inom förordningen. Arbetet har utförts genom att sammankoppla teori och en kvalitativ intervjuforskning. Utförde undersökningen med en intervju med en dataskyddsanvsarig för att undersöka hur förordningen påverkat ämbetsverk.

Resultatet visar att ämbetsverken vidtagit nya administrativa åtgärder för att öka säkerheten på behandling av deras kunders och anställdas personuppgifter. De har också ökat på åtgärder så att all information de samlar in går enligt lagen.

Språk: svenska

Nyckelord: dataskydd, GDPR, personuppgifter

Opinnäytetyö

Tekijä: Jennifer Lindholm

Koulutus ja paikka: Tradenomi, Vaasa

Suuntautuminen: Oikeushallinto

Valvoja: Mayvor Höglund

Otsikko: GDPR i praktiken – Dataskyddsförordningens påverkan på ämbetsverk

Päivämäärä: 18.11.2022 Sivuja: 35

Tiivistelmä

Digitalisaation ja sen nopean kehityksen vuoksi otettiin käyttöön tietosuoja-asetus. Asetus tuli voimaan toukokuussa 2018. Yleinen tietosuoja-asetus tuli voimaan henkilötietojen käsittelyn turvallisuuden lisäämiseksi ja sen varmistamiseksi, että luonnolliset henkilöt ovat turvassa henkilötietojensa ja niihin liittyvien oikeuksien suhteen. Viranomaiset, jotka käsittelevät henkilötietoja päivittäin, ja osa henkilötiedoista voi olla yksilöiden kannalta arkaluonteisia, joten on tärkeää, että asetuksen periaatteita noudatetaan kirjaimellisesti. Jos virastot eivät noudata asetusta, niille voidaan määrätä hallinnollinen sakko.

Tämän opinnäytön tarkoituksena on selvittää, miten virastot käsittelevät henkilötietoja, miten henkilötietoja kerätään ja minne ne päätyvät sekä mitä riskejä ja ohjeita asetus sisältää. Työ on toteutettu yhdistämällä teoriaa ja laadullista haastattelututkimusta. Toteutin tämän tutkimuksen haastattelemalla yhtä tietosuojavastaavaa selvittääkseen asetuksen vaikutusta virastoihin. Tulokset osoittavat, että virastot ovat toteuttaneet uusia hallinnollisia toimenpiteitä parantaakseen asiakkaidensa ja työntekijöiden henkilötietojen käsittelyn turvallisuutta. Ne ovat myös tehostaneet toimenpiteitä varmistaakseen, että kaikki niiden keräämät tiedot ovat lain mukaisia.

Kieli: Ruotsi

Avainsana: GDPR, tietosuoja, henkilötietoja

BACHELOR'S THESIS

Author: Jennifer Lindholm
Degree Programme: Business Administration
Specialisation: Administration of justice
Supervisor(s): Mayvor Höglund

Title: GDPR i praktiken – Dataskyddsförordningens påverkan på ämbetsverk

---

Date 18.11.2022 Number of pages 35 Appendices 1

Abstract

Due to digitalisation and its rapid development, a data protection regulation was introduced. The regulation came into force in May 2018. The GDPR came into force to increase the security of processing personal data and ensure the safety of natural persons regarding their personal data and the rights related to it.
Public authorities process personal data daily and some of the personal data may be sensitive to individuals, and, therefore it is important that the principles of the Regulation are followed to the letter. If agencies do not comply with the Regulation, they may be subject to an administrative penalty.

The purpose of this paper is to find out how agencies process personal data, how personal data is collected and where it ends up, and what the risks and guidelines are under the Regulation. The work has been carried out by combining theory and qualitative interview research. Carried out the research with an interview with a data protection officer to explore the impact of the regulation on agencies.

The results show that the agencies have taken new administrative measures to increase the security of the processing of their customers' and employees' personal data. They have also stepped-up measures to ensure that all the information they collect complies with the law.

Language: Swedish
Key words: GDPR, data protection, personal information

Innehållsförteckning

1 Inledning

GDPR är en förordning som togs i kraft i maj 2018 och togs fram för att öka säkerheten av behandling av personuppgifter. Denna förordning gjordes på EU:s direktiv och lägger större vikt på de företag och organisationer som behandlar EU medborgares personuppgifter. GDPR och dess lagstiftning är inte hemskt gammal och alla organisationer har måsta tillämpa sin verksamhet enligt dataskyddsförordningen.

Det behandlas enorma mängder personliga data av både privata och offentliga aktörer, detta gör att den nya förordningen blev väldigt viktig för företag och organisationer för att bättre kunna skydda sina kunders data. (Wendleby & Dag, 2019)

Denna Dataskyddsförordning togs i bruk för att stärka säkerheten på behandlingen av personuppgifter också för att tackla de utmaningar inom dataskyddet som digitaliseringen medför.

I detta arbete kommer man få en bättre syn på hur dataskyddsförordningen har tillämpats på den offentliga sektorn, i synnerhet på ämbetsverk som varje dag behandlar personuppgifter. GDPR har funnits en tid redan men fortfarande finns det företag som inte vet om alla följder som denna förordning medför.

1.1 Problemområde

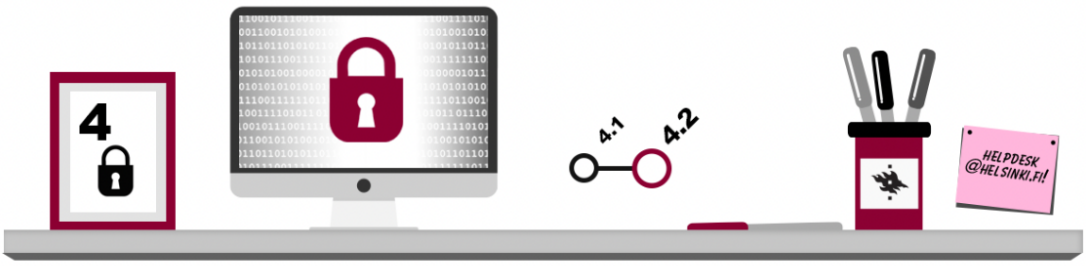
Vad finns det då för problem med dataskydd? Vanligtvis då man samlar in personuppgifter är att det mesta görs digitalt. När allting görs digitalt är problemet att personuppgifterna lätt sprider sig till fel händer. Dataskydd som har en stor roll och betydelse när man behandlar personuppgifter och någon annans känsliga information är det ytterst viktigt att kunna ta reda på varifrån problemen främst uppstår och utifrån det försöka förhindra att sådana olyckor inträffar. Några problem med dataskyddsfrågor är:

Ett problem är att det oftast uppkommer dataläckor. Och en dataläcka är ett resultat av ett dataintrång och med dataintrång menas när någon olovligen tagit sig i en tjänst eller någon

databas och fått tag på känslig information såsom personuppgifter. På yle.fi finns ett bra exempel på vad en dataläcka kan orsaka.

I en artikel på Yle.fi berättas det om Vastaamo-läckan där personbeteckningar hamnade i fel händer och det orsakades mycket konsekvenser för offren som var inblandade. Denna dataläcka skedde vid Östra Nylands universitet och utbildningsorganisationen Työtehoseura under åren 2018–2019. Under denna dataläcka hamnade 16 000 personbeteckningar i fel händer och användes av kriminella för att till exempel köpa varor på kredit på nätet. Och efter denna dataläcka har man nu försökt komma på nya sätt för att undvika att personbeteckningar eller personuppgifter i allmänhet inte skall spridas till fel händer. Detta är bara ett exempel på en dataläcka och vad en sådan kan orsaka. Men det finns många fler, dataläckor anses vara den största boven då det gäller dataskydd. (Fagerström, 2022)

Ett annat problem gällande dataskydd är sociala medier på grund av att under de senaste åren har nätkommunikationen blivit allt större och till en stor del tagit över den traditionella nätkommunikationen såsom epost. Nuförtiden använder sig man sociala medier såsom Facebook, Whatsapp, Instagram och Twitter. Denna sorts av kommunikationen används både privat och offentligt. Dock är det väldigt svårt att hålla all information hemlig, största problemet med sociala medier är att det lätt uppstår bedrägerier och skadeprogram, skadeprogram kan vara en länk som man skall klicka på som sedan skapar ett virus på telefonen som gör att telefonen blir lätt att hacka sig in på, ett annat exempel av skadeprogram är om någon anser sig vara från en tävling och vill att man skalla svara på massa frågor om privat information som kan leda till att de stjäl en persons känsliga information såsom bank ID-nummer eller personsignum. De flesta sociala medier har en massa sekretessinställningar men trots detta har en dels information och bilder hamnat i någon annans händer. Sociala medier anses då vara ett problem då det lämnas digitala fotspår efter en. Och på de senaste så har identitetsstölder blivit alltmer vanligt och därför borde man vara väldigt medveten om hurudan information man delar med sig på nätet. (Studentens Digitalkompetens, 2022)



Figur 1: Bilden beskriver hur många olika sätt det finns att skydda sin information från att den inte skall hamna i fel händer. Källa: Helsingfors universitet

I detta arbete kommer jag mera att sätta fasta på problemen som kretsar kring dataskyddsförordningen GDPR och hur den har påverkat företag i allmänhet, hur förordningen har satt sin prägel på företags arbetsprocesser med tanke på alla problem som förekommer i den digitala världen.

1.2 Syfte

Syftet med detta arbete är att undersöka hur ämbetsverk har anpassat sig till EU:s dataskyddsförordning och hur förordningen har påverkat deras sätt att arbeta. För att nå fram till mitt syfte kommer jag att måsta undersöka hur ämbetsverken behandlar personuppgifter och hur de har tillämpat den nya dataskyddsförordningen.

Mina forskningsfrågor är:

Hur har ämbetsverk påverkats av GDPR?

Hur har förordningen påverkat arbetsprocessen?

Vad finns det för följder och risker om dataförordningen inte följs?

1.3 Avgränsning

Jag kommer i detta arbete avgränsa mig till att titta mer på ämbetsverk och hur de har påverkats av denna förordning och hur de anser att förordningen varit sedan den trädde i kraft 2018.

1.4 Metod

Som metod för detta arbete kommer jag till den teoretiska delen använda mig ut av litteratur där jag läser mig in mer om GDPR och vad GDPR betyder i praktiken. Till den empiriska delen kommer jag att använda mig av en kvalitativ metod.

I detta arbete använde jag mig av en kvalitativ och en rättsdogmatisk metod. Jag både intervjuade ämbetsverks dataskydds ansvariga och sedan analyserade och tolkade jag dataskyddsförordningen för att komma fram till resultatet. Och på detta sätt fick jag reda svaret på hur GDPR påverkat ämbetsverk i praktiken.

Jag valde mig att använda en kvalitativ forskning för detta arbete och detta gjorde jag genom att utföra en intervju och valde att göra en strukturerad intervju vilket betyder att jag före intervjun skrivit färdiga frågor och utifrån detta genomförde jag intervjun. Jag ansåg att jag genom detta fick svar på exakt det jag ville undersöka i mitt arbete.

1.5 Disposition

I kapitel 1 kommer min inledning att vara där det redogörs vad arbetet kommer att handla om och i kapitlet redogörs också problem och syftet med arbetet.

I kapitel 2 redogörs det om GDPR i allmänhet, kapitlet tar upp en beskrivning på vad GDPR är och där förklaras också begrepp som hänger ihop med GDPR och självaste dataskyddsförordningen.

I kapitel 3 behandlas regleringen av GDPR, med andra ord vilka lagar som berör GDPR. Och i detta arbete så har jag främst tagit och behandlat Dataskyddslagen och självaste Dataskyddsförordningen från EU.

I kapitel 4 finns intervjun där frågorna och svaren behandlas skilt för sig.

I kapitel 5 redogörs en analys av resultatet och i kapitlet hålls också slutdiskussionen av mitt arbete.

I kapitel 6 sammanfattas arbetet med att jag besvarar mina egna forskningsfrågor.

2 Allmänt om GDPR

GDPR är en förkortning av General Data Protection Regulation och trädde i kraft den 25 maj 2018 i alla EU-länder. (Dataskydd, 2022)

Syftet med denna dataskyddsförordning var att ge bättre skydd för personuppgifter, ge fler metoder för att administrera egna uppgifter, för att kunna tackla utmaningar inom dataskyddet som digitaliseringen medför samt att utveckla EU:s inre marknad. Och GDPR berör alla företag och organisationer som behandlar personuppgifter.

Företag och organisationer har mycket att ta hänsyn till då GDPR skall tillämpas, rent praktiskt betyder det att företag och organisationer måste ta följande saker i beaktande:

- De får inte samla in fler personuppgifter än vad som är nödvändigt
- Datat får inte sparas längre tid än nödvändigt
- Det skall vara bestämt i förväg vad datat skall användas till
- Det skall finnas rättslig grund för datahantering, som t.ex ett avtal
- Personuppgifterna skall hållas korrekta, uppdaterade och får inte sparas utanför EU eller utanför länder med samma lagstiftning
- Alla registrerade personer har rätt att veta vad för data som sparats och vad den används till, registrerade personer har också rätt att raderas och bli bortglömda
- Det skall finnas skriftlig dokumentation över hur personuppgifterna hanteras
- Leverantörer skall också följa GDPR om de hanterar personuppgifter
- Alla säkerhetsincidenter som t.ex dataintrång måste anmälas till Datainspektionen. (Hur påverkar EU:s dataskyddsförordning (GDPR) företag och organisationer?, 2022)

Figur 2: På bilden finns det utritat kategorierna av GDPR.

Källa: Solatum.se

2.1 Personuppgifter

Vad är personuppgifter? Det finns många definitioner på vad en personuppgift är. En definition från boken GDPR- Förstå och tillämpa i praktiken är definitionen den att personuppgifter är allt som avser en identifierad eller identifierbar fysisk person.

En identifierbar fysisk person är någon som kan direkt eller indirekt kan identifieras, detta kan vara till exempel ett namn, ett personnummer. En person kan också identifieras av en eller flera faktorer som är specifika för en persons fysiska, fysiologiska, genetiska, psykiska, biometriska, ekonomiska, kulturella eller sociala identitet. (Wendleby & Dag, 2019)

Personuppgifter kan också vara subjektiva och objektiva. I boken GDPR- Förstå och tillämpa i praktiken förklaras subjektiva och objektiva så här: objektiva personuppgifter är det som man oftast tänker på först, dessa personuppgifter beskriver någon såsom; namn, adress, personnummer och telefonnummer. Subjektiva personuppgifter är i sig mera beskrivande av egenskaper. Subjektiva personuppgifter beskriver en eller flera faktorer som

beskriver den fysiska personens fysiska fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Dataskyddsförordningen gäller endast behandling av personuppgifter av personer som fortfarande är levande, vilket betyder att de personer som enligt lag anses avlidna omfattas inte av dataskyddsförordningen.

Figur 3: På denna bild finns det uppräknat exempel på vad en personuppgift kan vara. Källa: samlogic.com

2.1.1 Behandling av personuppgifter

Till att börja med, när personuppgifter börjar behandlas tillämpas främst dataskyddsförordningen och dataskyddslagen. Det finns fem delar av behandling av personuppgifter: inhämtning, lagring, hantering, delning och gallring. (Wendleby & Dag, 2019)

Inhämtning	Lagring	Hantering	Delning	Gallring
Insamling	Lagring	Bearbetning	Överföring	Lagring
Framtagning		Ändring	Spridning	Radering
Registrering		Läsning	Tillhandahållande	Förstöring
		Användning		
		Justering		
		Sammanförande		
		Strukturering & Organisering		
		Begränsning		

Figur 4: På denna bild finns det uppräknat de olika sakerna som hör till de fem olika delarna av behandling av personuppgifter.

För att dataskyddsförordningen skall tillämpas måste varje behandling av personuppgifter vila på en laglig grund. I boken GDPR- Förstå och tillämpa i praktiken finns det sex lagliga grunder uppräknade och för att förordningen skall tillämpas måste alltid en eller flera av grunderna stå som grund vid behandling av personuppgifter. De sex lagliga grunderna är:

1. Den registrerade har gett sitt samtycke till att hens personuppgifter behandlas för ett eller flera specifika ändamål.
2. Behandlingen är nödvändig för att fullgöra ett avtal.
3. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse.
4. Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerande.
5. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

6. Behandlingen är nödvändig för ändamål som berör den personuppgiftsansvariges intressen, om inte den registrerades intressen eller grundläggande rättigheter väger tyngre

All behandling av personuppgifter skall göras lagligt och på rätt sätt. För att behandla andras personuppgifter måste ämbetsverk gå enligt de principer som finns skrivna i dataskyddsförordningen i artikel 5 och 6. De sju principerna som ämbetsverken måste gå enligt är:

1. Laglighet, korrekthet och öppenhet.

2. Ändamålsbegränsning, med detta menas att uppgifter skall samlas in för särskilda, uttryckligt angivna och berättigade ändamål.

3. Uppgiftsminimering, vilket betyder att uppgifterna ska vara adekvata, relevanta och inte för omfattade i förhållande till det ändamål de behandlas.

4. Uppgifterna skall vara riktiga och uppdaterade.

5. Lagringsminimering, med detta menas att uppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt

6. Integritet och konfidentialitet, med detta menas att uppgifterna skall behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna och med användning av lämpliga tekniska och organisatoriska åtgärder

7. Ansvarsskyldighet, den som är ansvarig för personuppgifter skall se till att föregående principer uppfylls. (EU:s dataskyddsförordningen, 2022)

2.2 Den registrerades rättigheter

Jag berättade tidigare lite om vad GDPR är i praktiken och nu tänkte jag mera konkretisera vilka rättigheter vid behandling av personuppgifter.

Som privatperson har man rätt att få information om behandlingen av personuppgifterna, få tillgång till sina egna personuppgifter, rätta uppgifter, avlägsna uppgifter och man har rätt att bli glömd, rätt att begränsa behandlingen av sina personuppgifter, flytta sina uppgifter mellan olika system, man har också rätt att göra en invändning mot behandling av sina personuppgifter och man har också rätt att inte bli föremål för automatiskt beslutsfattande.

Rätt till information betyder att den registrerade har rätt att få information när uppgifterna samlas in samt när den registrerade begär om de. Information skall också ges till den registrerade då till exempel ett dataintrång eller en personuppgiftsincident inträffar och det finns risk för bedrägeri eller identitetsstöld. Denna information skall ges gratis o en lättillgänglig och skriftlig form, elektronisk form gäller också, viktigast är att informationen är skrivet med ett klart och tydligt språk. (Integritetsskyddsmyndigheten, 2022)

Den registrerade har bland annat rätt till att få veta:

- Till vilka ändamål informationen skall användas till
- Vad den rättsliga grunden är för behandlingen
- Hur länge uppgifterna kommer att lagras
- Har rätt att få veta att man har rätt att lämna klagomål

Rätt till tillgång betyder att den registrerade har rätt att vända sig till personuppgiftsansvarige för att få veta om den registrerades uppgifter behandlas eller ej. Om uppgifterna behandlas skall det ges ett dokument som innehåller följande information. Till vilka kategorier personuppgifterna behandlas, till vad uppgifterna används för, hur länge de kommer sparas, vilka av dessa uppgifter som delats och varifrån uppgifterna kommer. Dock kan det uppkomma omständigheter som medför att informationen inte får lämnas ut och detta kan vara om bestämmelser i någon annan lag som strider mot det. (Integritetsskyddsmyndigheten, 2022)

Rätt till rättelse betyder att den registrerade har rätt att be om att få felaktiga uppgifter rättade, det innebär också att man har rätt att komplettera sådana uppgifter som saknas eller som är relevanta till ändamålet. (Integritetsskyddsmyndigheten, 2022)

Man har också rätt att bli raderad, med detta menas att man som registrerad kan be om att uppgifterna raderas i bland annat följande fall

- Om uppgifter inte behövs mera
- Om behandlingen grundar sig på registrerades samtycke och denna sedan återkallar samtycket
- Om uppgifterna används för direktmarknadsföring och den registrerade motsätter att uppgifterna skall användas till detta
- Om uppgifterna behandlas olagligt

För att den registrerade har rätt till radering måste den fylla en rättslig skyldighet. Men med allting finns det undantag och samma gäller här. (Integritetsskyddsmyndigheten, 2022)

Rätt till att begränsa behandlingen av personuppgifter betyder att som registrerad har man rätt att ibland kräva att behandlingen av personuppgifter skall begränsas och med begränsning betyder att uppgifterna endast får användas för vissa syften i framtiden. Och begränsning gäller då den registrerades uppgifter varit felaktiga och sedan bett om rättelse. (Integritetsskyddsmyndigheten, 2022)

Rätt att göra invändningar betyder att man har rätt att invända vid behandling av personuppgifter då det gäller behandling av en uppgift av allmänt intresse eller myndighetsutövning. Om en registrerad gör en invändning måste det finnas avgörande berättigade skäl för detta. Dock då invändningarna gäller direktmarknadsföring har den registrerade alltid rätt att invända. (Integritetsskyddsmyndigheten, 2022)

Rätt att få flytta information mellan olika system betyder i det stora hela att man har rätt använda sina personuppgifter på annat håll som exempel på sina egna sociala medier. (Integritetsskyddsmyndigheten, 2022)

Sista rätten att man har rätt att inte bli föremål för automatiserade beslut kan vara ett automatiserat avslag på en kreditansökan som gjorts på internet eller ett nekande besked från

e-rekrytering utan någon personlig kontakt. Ända gången detta kan vara tillåtet är om det är nödvändigt för att ingå eller fullgöra ett avtal. (Integritetsskyddsmyndigheten, 2022)

Alla rättigheter som den registrerade har förverkligas inte i alla situationer**,** kommer göra en tabell nedan där det förklaras närmare vilka rättigheter som används i vilka situationer**.** Rättigheterna kommer vara i den lodräta kolumnen och situationerna kommer att vara på den vågräta raden (Integritetsskyddsmyndigheten, 2022)

Tabell över situationer där rättigheterna används olika. Tabellen har gjorts för att lättare förklara när och vid vilka situationer den registrerades rättigheter kan användas eftersom att alla rättigheter inte tillämpas i alla situationer.

	Rättigheter då ett sam-tycke av den registrerade ligger grund för behandling	**Rättigheter då grunden för behandling utgörs av ett avtal**	**Rättigheter då behandlingsgrunden utgörs av lagstadgade plikter för den personuppgifts-ansvarige**	**Rättig-heter då grunden för behandlingen utgörs av ett vitalt intresse för en registrerad person**	**Rättig-heter då grunden för behandling är en uppgift som gäller ett allmänt intresse eller offentlig makt**	**Rättigheter då behandlingsgrunden utgörs av ett berättigat intresse hos den personuppgiftsansvarige**
Rätten att få information om	X	X	X	X	X	X

behandling av personuppgifter						
Rätten till tillgång till uppgifter	X	X	X	X	X	X
Rätten att rätta uppgifter	X	X	X	X	X	X
Rätten till borttagning av uppgifter	X	X		X		X
Rätten att begränsa behandlingen av uppgifter	X	X	X	X	X	X
Anmälningsskyldighet som gäller rättelse eller begränsning	X	X	X	X	X	X
Rätten att flytta uppgifterna mellan system	X	X				
En registrerad	X					

kan tillåta automatiskt beslutsfattande med ett uttryckligt samtycke						
Rätten att inte vara föremål för automatiskt beslutsfattande UTAN lagenlig grund		X	X (detta kan möjliggöras med lagstiftning där behöriga åtgärder fastställs för att skydda de registrerades rättigheter och friheter		X	
Rätten att göra invändning mot behandling av uppgifter					X	X

2.3 Risker och följder

Med allting finns det för och nackdelar, med GDPR finns det mycket positivt speciellt då GDPR gäller säkerheten av våra personuppgifter men med detta följer ett stort ansvar för ämbetsverken. För ämbetsverk är det viktigt att följa de riktlinjer och principer som lagts eftersom följs inte principerna medför det stora påföljder för ämbetsverken.

Om bolag går emot de principer som lagts mot behandling av personuppgifter kan de få höga sanktionsavgifter. Bolag kan få betala böter upp till 20 miljoner euro eller 4 % av bolagets globala omsättning. Vid lägre sanktionsnivå kan boten vara 10 miljoner euro eller 2 % av den bolagets globala omsättning. När räknas det som högre eller lägre sanktionsnivå, detta kommer jag att lista upp till följande.

Högre sanktionsnivå gäller:

- Då de grundläggande principerna för behandling inte följs
- De registrerades rätt till information, rättelse eller radering inte följs
- Behandling av känsliga personuppgifter inte följs
- Överföring av uppgifter till en tredje part utan adekvat skyddsnivå
- Inte följt förelägganden från Datainspektionen

Lägre sanktionsnivå gäller:

- Då vissa regler gällande dataskydd vid skyldighet att föra behandlingsregister eller göra konsekvensbedömning inte följs
- Då allmänna krav som gäller för personuppgiftsansvariga och biträden inte följs
- Vid dataskyddsombud

I boken har det på s 459 räknats upp ett bra exempel angående dessa avgifter. Exemplet gällde Heathrowflygplats som fick en sanktion på 120 000 pund för att det förlorat ett USB-minne som innehöll några filer med personuppgifter. USB-minnet var inte krypterat eller skyddat med något lösenord men ändå fick flygplatsen en sanktion. Orsaken till denna incident ansågs vara att personalen inte var tillräckligt utbildad och att det inte fanns tillräckligt med skyddsåtgärder som kunde hindra nedladdningen av personuppgifterna på USB-minnet (Wendleby & Dag, 2019)s.459

När det händer något i företag och personuppgifter sätts i fara kallas dessa händelser för personuppgiftsincidenter. I boken (Wendleby & Dag, 2019) på sidorna 440–442 står det skrivet om personuppgiftsincidenter och när och till vem dessa skall anmälas.

Till att börja med en personuppgiftsincident är enligt dataskyddsförordningen en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller som leder till obehörigt röjande/ obehörig åtkomst till de personuppgifter som behandlats. Begreppet förlust omfattar situationerna när personuppgifterna förstörts eller när organisationen inte längre kan komma åt uppgifterna. Begreppet förstöring omfattar situationen när personuppgifterna har ändrats, korrigerats, blivit korrumperade eller som inte längre är kompletta. Det sista begreppet obehörighet röjande betyder avslöjande av personuppgifter till mottagare som inte har behörighet att använda sådana personuppgifter.

Ett bra exempel på detta är då en mobil enhet eller bärbar dator som innehåller en organisations kunddatabas stjäls eller tappas bort. I artikel 29 i förordningen stor det skrivet att säkerhetsincidenten måste innehålla personuppgifter för att dataskyddsförordningen skall gälla. (Wendleby & Dag, 2019)

Om en personuppgiftsincident inträffas skall den drabbade personuppgiftsansvarige dokumentera incidenten och anmäla denna till Datainspektionen inom 72 timmar. Viktigt att komma ihåg är att anmälan skall göras utan dröjsmål men organisationen har ändå de 72 timmarna på sig att meddela om incidenten. (Wendleby & Dag, 2019)

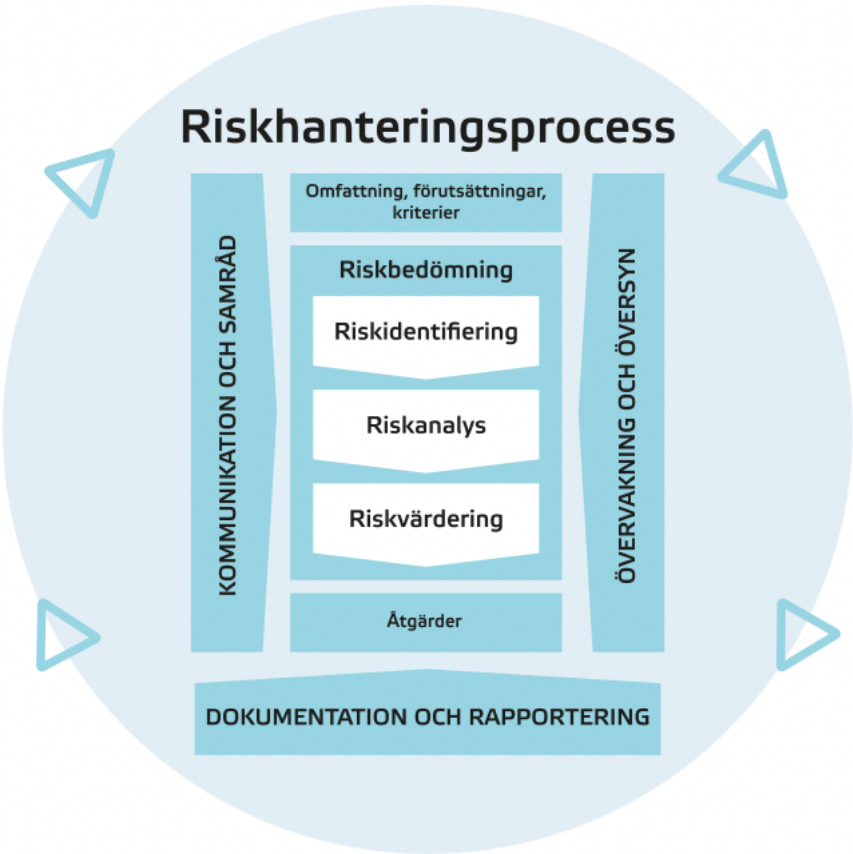
Då man vill minimera chanserna med risker utför man en så kallad riskbedömning. Till riskbedömningen hör fyra delar: identifiera, analysera, värdera riskerna samt förstå riskerna. Riskhantering är en systematisk process där meningen är att identifiera problemet, analysera detta och värdera riskerna med problemet samt att till slut förstå sig på självaste problemet. Riskhanterings kriterierna väljs utifrån organisationens värderingar, egna mål och dess resurser. (Boverket, 2022)

De olika delarna förklarade per begrepp. Den första delen identifiera betyder att man skall som namnet säga identifiera riskerna, och för att identifiera riskerna kan man göra en

bruttolista som kan innehålla arbetsmoment som kräver stor noggrannhet vid utförandet av detta arbetsmoment. Denna lista skall också innehålla vanligt kommande fel, brister och skador om sådana finns. (Boverket, 2022)

Nästa steg som är analysera betyder att man tydligt skall beskriva riskerna utifrån bruttolistan för att sedan kunna bedöma riskerna och hur dessa risker uppstår samt vilka konsekvenser som kunde uppkomma om riskerna sker. Självaste syftet med analysdelen är att man skall förstå riskens karaktär och egenskaper. Genom att göra denna del får man ett bra underlag för nästa del och gör det lättare att göra beslut om hur riskerna behöver hanteras och hur. (Boverket, 2022)

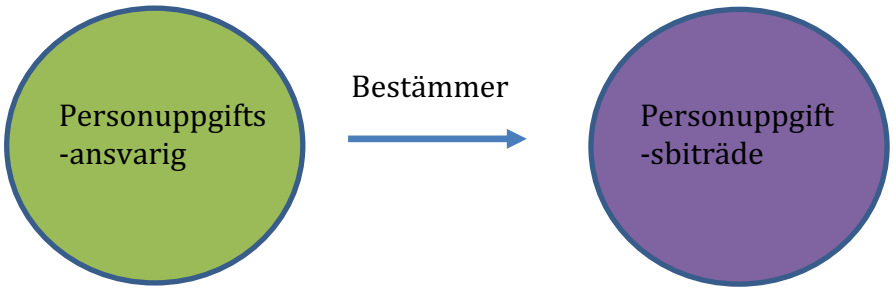
Tredje steget, värdera riskerna. Syftet med denna del är att vara som ett stöd vid slutskedet då det är dags att göra ett beslut om vilka åtgärder som måste utföras för att riskerna skall kunna undvikas. Vid värdering av riskerna jämför man resultatet från analysdelen med riskkriterierna för att på det sättet fastställa riskernas relevans. Till allra sist är det viktigt att verkligen förstå riskerna och de åtgärder som verkligen måste tas. (Boverket, 2022)



Figur 5: På bilden visas riskhanteringsprocessen steg för steg och sammanfattar vad den hela processen består av. Källa: Boverket.se

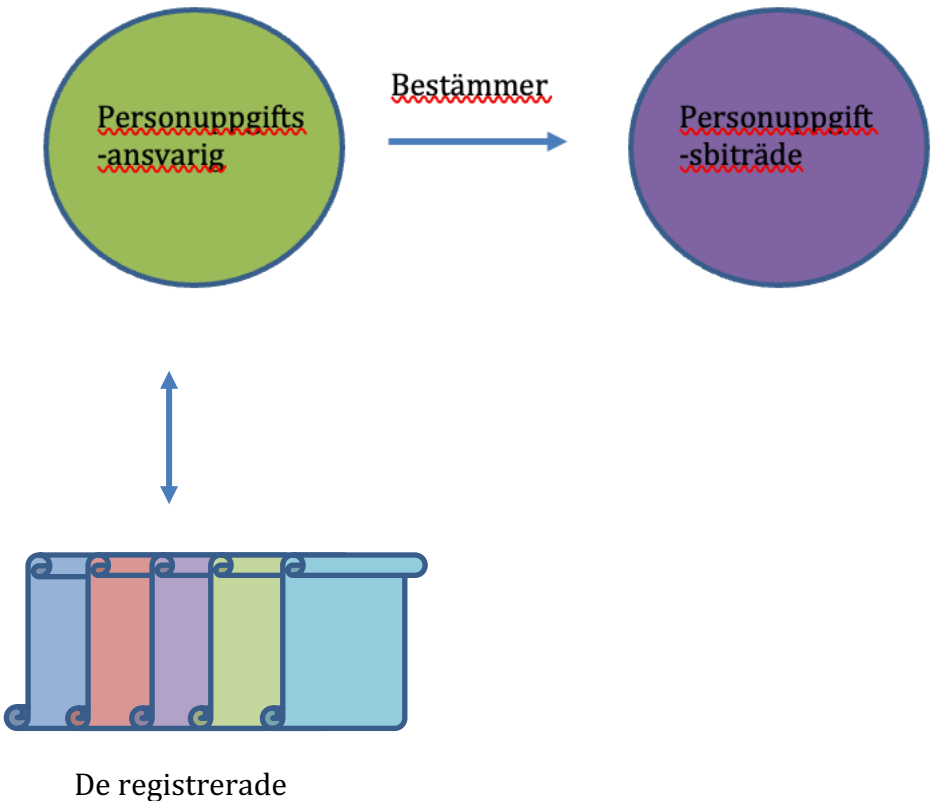
2.4 Organisatoriska krav

För att GDPR:s principer och regelverk skall kunna tillämpas till det bästa hos organisationer skall det finnas personuppgiftsansvariga och personuppgiftsbiträden. Detta är reglerat i dataskyddsförordningen i artikel 32. En personuppgiftsansvarig kan vara en fysisk eller juridisk person, offentlig myndighet eller ett organ som själv eller tillsammans med andra bestämmer ändamålen och medlen för den bästa behandlingen av personuppgifter. Personuppgiftsbiträden kan vara de samma som personuppgiftsansvariga ända skillnaden mellan dessa två är att biträden blir anställda av personuppgiftsansvariga och utför det arbetet som de ansvariga vill att skall utföras. (Wendleby & Dag, 2019)



Figur 6 förklarar förhållandet mellan personuppgiftsansvarige och personuppgiftsbiträdet.

Ovanstående figur förklarar förhållandet mellan de båda och visar hur det är de ansvariga ger instruktioner åt biträdena som de sedan skall följa. Nästa figur kommer att förklara att det är den personuppgiftsansvarige som skall säkerställa att det alltid finns tydliga ändamål och laglig grund för behandling av den registrerades personuppgifter. (Wendleby & Dag, 2019)



Figur 7 förklara hur personuppgiftsansvarige fungerar som en kontaktperson med de registrerade och hur personuppgiftsansvarige i sin tur är i kontakt med personuppgiftsbiträdet.

Andra organisatoriska åtgärder som också införskaffats på grund av dataskyddsförordningen är tekniska säkerhetsåtgärder och tekniskas säkerhetsåtgärder är t.ex

- Inloggning
- Behörighets spärrar
- Brandväggar
- Antivirus
- Säkerhetskopiering
- Kryptering

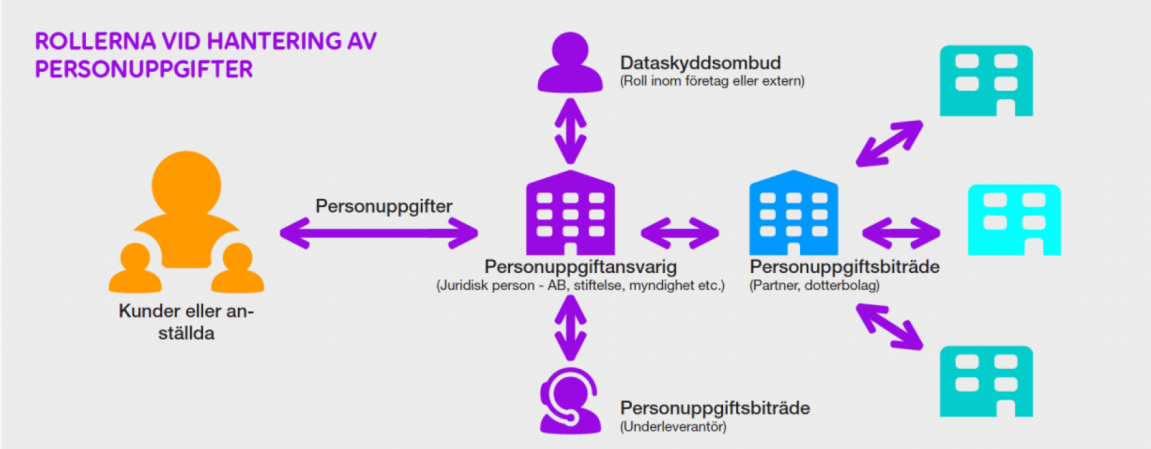
Dessa tekniska åtgärder infördes för att kundernas och personalens personuppgifter skall hållas så säkra som möjligt och minska risker som hackning. (Säkerhet, 2022)

2.4.1 Dataskyddsombud

Organisationer brukar oftast ha ett dataskyddsombud och denna skall informera och ge råd till organisationen om vilka skyldigheter som finns i dataskyddsförordningen och vad dess lagstiftning är. Ombudet kan vara en anställd eller en extern resurs. Ombudets största roll är att kontrollera och övervaka om det sker några förändringar som måste tillämpas i organisationens verksamhet. (Wendleby & Dag, 2019)

På dataombudsmannens webbsida kan man läsa mera om en dataskyddsombuds uppgifter mera specifikt och på hemsidan är dataombudsmannens arbetsuppgifter följande:

- Skall följa efterlevnaden av dataskyddsbestämmelserna i hela organisationen och sedan lyfta fram brister som upptäckt
- Skall ge information och råd om skyldigheterna till ledningen och arbetstagarna som behandlar personuppgifter
- Skall på begäran ge råd om hur konsekvensbedömningen skall göras och övervakar sedan genomförandet av detta
- Dataskyddsombudet är också kontaktperson för de som är registrerade och hjälper i ärenden som gäller behandling av personuppgifter (Dataskyddsombud, 2022)



Figur 8: Bilden förklara bättre bild hur sambandet mellan alla dessa organisatoriska kravv som infördes och hur samarbetet mellan kunderna och personuppgiftsansvarige sköts.

Källa: GDPRcert.se

3 Regleringen av GDPR

GDPR styrs av självaste dataskyddsförordningen men GDPR går också efter dataskyddslagen och upphovsrättslagen. I detta kapitel kommer jag gå in lite mera på lagstiftningen gällande GDPR.

3.1 Europaparlamentets och rådets förordning

Denna förordning är grunden för hela GDPR och dataskyddslagen. Förordningen tillämpas endast då det gäller behandling av personuppgifter. Denna förordning är lång och är uppdelat i kapitel och artiklar. I detta arbete har jag mest tittat på kapitel 1–4, och 8. Dessa kapitel handlar om allmänna bestämmelser, principer, den registrerades rättigheter, personuppgiftsansvarig och biträden och rättsmedel, ansvar och sanktioner. Denna förordning går ganska bra hand i hand med Dataskyddslagen (1050/2018) så dataskyddslagen innehåller i stort setts amma sak som förordningen men i en mera kortfattad helhet. För att lite kortfattat beskriva kapitlen och de avsnitten som jag ansett vara viktiga för just min undersökning och som jag hänvisar till då jag talar om förordningen. (EU:s dataskyddsförordningen, 2022)

Kapitel 1 artikel 1 beskriver syftet med förordningen. Syftet med förordningen är att fastställa bestämmelser om skydd för fysiska personer gällande behandlingen av deras personuppgifter. Förordningen vill också skydda fysiska personers grundläggande rättigheter. Artikel 2 och 3 behandlar de tillämpningsområden där förordningen tillämpas, förordningen tillämpas vid behandling av personuppgifter som helt eller till en del företas på automatisk väg samt på personuppgifter som förekommer i något register.

I förordningens andra kapitel är principerna beskrivna men dessa har jag redan nämnt tidigare i detta arbete i kap 2.1.1.

I förordningen tredje kapitel avsnitt 1 står det skrivet om de registrerades rättigheter gällande insyn och villkor. I avsnitt 2 står det skrivet om information och tillgång till personuppgifter.

I avsnitt 3 handlar det om rättelse och radering och i det 5 och sista avsnittet är begränsningar där det räknas upp alla de begränsningar som finns vid behandling av personuppgifter och några exempel på då det finns begränsningar vid de registrerades rättigheter är om man vill säkerställa den nationella säkerheten, försvaret eller den allmänna säkerheten, detta är bara några exempel men dessa känns mest relevanta för detta arbete.

I kapitel 4 handlar det om personuppgiftsansvarig och personuppgiftsbiträde och i detta kapitel räknas det upp allmänna skyldigheter som dessa har och vad dessa två är. (avsnitt 1–2, artiklarna 24–33)

I kapitel 8 beskrivs det om rättsmedel, ansvar och sanktioner, i detta kapitel tog jag mera och tittade på artiklarna 82–84 för att kunna ta och undersöka en av mina forskningsfrågor. (Integritetskydds myndigheten, 2022)

3.2 Dataskyddslag 1050/2018

I dataskyddslagen är syftet är att precisera och komplettera Europaparlamentets och rådets förordning om skydd av fysiska personer med betoning på behandling av personuppgifter. Dataskyddslagen tillämpas i enlighet med tillämpningsområdet i artikel 2 i förordningen. Denna lag tillämpas på alla slags arbeten förutom på riksdagsarbete eller när det gäller brottmål. Detta är stadgat i lagens 1 kap. 2§. (Dataskyddslag, 2022)

Dataskyddslagen trädde i kraft 1 januari 2019 och då denna lag trädde i kraft upphävdes personuppgiftslagen (523/1999) och lagen om datasekretessnämnden och dataombudsmannen (389/1994).

I lagens andra kapitel beskrivs de rättsliga grunderna för behandling av personuppgifter.

I kap 6 i lagen står det skrivet om särskilda bestämmelser som lagen medför, den bestämmelsen som är mest viktig från GDPR:s synvinkel är § 35, paragraf 35 är tystnadsplikt vilket betyder den som vid utförandet av åtgärden har fått reda på information

gällande den andra personen och med detta medför tystnadsplikt vilket i praktiken betyder att man inte får dela vidare informationen och man får inte använda informationen för någon annans vinning eller för att skada någon annan.

4 Resultat

I detta kapitel beskrivs resultatet av undersökningen, här står det skriver om intervjun och dess frågor samt svar på dessa. I kapitlet behandlas det också frågorna på ett djupare plan och frågorna besvaras var och en skilt för sig.

4.1 Intervjun

För att få svar på mina forskningsfrågor valde jag att ta och intervjua dataskyddsansvariga på ett ämbetsverk för att sedan kunna jämföra med dataförordningen och komma fram till ett resultat.

Jag hade en intervju med Tullens dataskyddsansvarige. Intervjun utfördes på distans och detta var en strukturerad intervju. I arbetet har jag valt att ha frågorna skilt och analysera varje fråga var för sig. Tullens dataskyddsansvariga kommer att kallas för X i detta arbete.

4.2 Val av ämbetsverk

Jag valde Tullen som ämbetsverk eftersom Tullen behandlar personuppgifter dagligen på från Finland men också från andra länder och tyckte det kunde vara intressant att veta hur de har blivit påverkade av den nya dataskyddsförordningen. Tullen är då ett ämbetsverk som resultat styrs av finansministeriet och samarbetar med näringslivet.

4.3 Insamlade datan

1. **Hur har GDPR-förordningen beaktas i er verksamhet? (Miten GDPR-asetus on otettu huomioon yrityksessänne?)**

   Med denna fråga ville jag få fram hur GDPR har tagits fram, hur förordningen påverkat det stora hela. Och om förordningen tagit fram extra åtgärder. Hennes svar var att följande, efter att dataskyddsförordningen togs i bruk 2016 så började ett

dataskyddsprojekt där Tullen kartläggde behovet av åtgärder och utvecklingsåtgärder. Efter dethär är dataskyddet inbyggt i Tullens uppbyggnad, helhets arkitekturen, tjänsteutvecklingen och det är del av deras bevisskyldighet. Tullen såg på GDPR mera som en administrativ sak såsom att de ändrade deras verksamhetsplan utifrån det som måste tillämpas från dataskyddsförordningen.

2. **Har dataskyddsförordningen varit hjälpsam och har den medfört någraslags förmåner? Om ja isåfall hurudana? (Onko tietosuoja-asetuksesta ollut hyötyä ja onko se tuonut jonkunlaisia etuja? Jos on niin millaisia?)**

Med denna fråga ville jag ta reda på om X hade sett något positivt i och med förordningens införande och om hon ansåg att den fört med sig förmåner av något slag. X svarade följande att förordningen på en EU-nivå har gjort det möjligt för Tullen att ha en stark grund för en horsiontal behandling av personuppgifter. Ramarna för samarbetet mellan EU-medlemsstaterna har varit klara, efetrsom alla medlemsländer tillämpar Dataskyddsförordningen.
Svaret jag fick var väldigt vagt och enligt X har GDPR bidragit med mera samarbete mellan EU-medlemsländer då det gäller behandling av personuppgifter, det gör Tullens arbete lättare då andar länder har liknande regler och principer.

3. **Har dataskyddsförordningen medfört några nackdelar? Om ja hurudana? (Onko tietosuoja-asetuksesta ollut haittaa? Jos on niin millaisia?)**

Me denna fråga ville jag ta reda på om GDPR medfört negativa följder på arbetsprocessen. X tyckte att för Tullen har dataskyddsförordningen i sig inte medfört några nackdelar men det har kommit som önskemål att dataskyddsförordningen skulle kunna ge klarare verktyg till behandling av olika dataskyddsfrågor. Med detta menade X att det kunde finnas ett system som kunde behandla olika dataskyddsfrågor på samma ställe och inte fler olika system.

4. **Får eran personal någonslags utbildning inom ämnet? (Saako teidän henkilöstönne jonkunlainen koulutus tietosuojaan?)**

   Med denna fråga ville jag ta reda på om personalen blev utbildad i dtaskydd förän de börjar arbetet och om de får reda på följderna om dataskydds principerna inte följs. X svarade att jo på Tullen hör dataskydd med i deras introduktion och inlärning och de erbjuder också andra dataskyddskurser vid behov. Tullen är aöötså väldigt aktiva då det gäller att skola deras personal och se till att de vet vad som måste vetas.

5. **Vem har tillgång till kundernas personuppgifter och vem får använda vad? (Kenellä on pääsy asiakkaiden henkilötietoihin ja kuka voi käyttää mitä?)**

   I frågan ville jag mera veta om alla i personalen har tillgång till alla personuppgifter om deras kunder. X ville inte gå in på detaljer men X svaraade att inom deras organisation går tillträdesrättigheterna enligt vilka arbetsuppgifter var och en har, ingen har tillgång till sådana uppgifter som man själv inte behandlar.

6. **Har GDPR blivit dyrt för er på något sätt? (Onko GDPR tullut kalliiksi teille?)**

   Att tillämpa dataskyddsförordningen i sig har inte medfört några kostnader säger dataskyydsansvarige på Tullen eftersom det redan innan förordningen tillämpades en lag om personuppgifter. Dataskyddsförordningen har dock kanske ökat behovet av tilläggsresurser som t.ex en dataskyddsansvarig.

7. **Vad är din egen åsikt om dataskyddsförordningen? (Millainen on sinun oma mielipiteesi tietosuoja-asetuksesta?)**

   Sista frågan jag ställde X var vad hennes egna åsikt var och svaret var väldigt ärligt. X svar var att dataskyddsförordningen verkligen har medfört mera klarhet i deras sätt att behandla personuppgifer. X tycker att det är väldigt bra att behandlarens roll har fått mera betydelse och X tycker också att det är bra att avtalskraven finns till

pågrund av att det leder till mindre missförstånd eller till avtalsbrott. Men X menar också att just nu finns det mycket frågor gällande länder utanför EU, och på vilka grunder man skulle kunna behandla personuppgifter på personer från dessa länder. X kunde själv inte svara på hur länder utanför EU skulle kunna tillämpas i dataskyddsförordningen.

5 Analys och slutdiskussion

Ut av den insamlade datan och teorin kan jag se att dataskyddsförordningen inte har påverkat ämbetsverk så hemskt mycket eftersom ämbetsverken redan tidigare följt lag om behandling av personuppgifter så för ämbetsverk var det till en början inte mycket som måste tillämpas, dock genom att digitaliseringen går vidare i rask takt har också ämbetsverk hamnat anpassa sig ännu mer.

Åtgärder som ämbetsverket hamnat göra med införande av dataskyddsförordningen var att lägga till några nya resurser såsom en dataskyddsanvsarig och ett dataskyddsbiträde. Men införandet av detta har inte ökat kostnaderna för ämbetsverk i det stora hela utan införandet av GDPR ökade i stället det administrativa arbetet, detta beror ju såklart på de alla principer som medföljde då GDPR tillämpades. I intervjun och det som jag tagit från teorin jag forskat i så inser jag att de flesta ämbetsverk har lagt dataskydd som en viktig punkt i deras arbetsprocesser. Ämbetsverk arbetar med kort som funkar som deras ”hjärna” kan man säga, man kommer inte åt någon information utan att man har ett organisationskort som kan identifiera vem man är. Jag som själv jobbar på ett ämbetsverk vet att man utan organisationskortet så slipper man inte på arbetsdatorn. Detta har nog gjort att behandlingen av personuppgifter har säkrats väldigt mycket och detta leder till att personen har mycket mindre chans att hamna i fel händer.

Utifrån denna undersökning lärde jag mig att ämbetsverk inte avvikit så hemskt mycket från hur de förr gick till väga utan att ämbetsverk mera lagt en större tyngd på självaste ämnet dataskydd och att man ökat säkerheten då det gäller behandling av andras personuppgifter. Dock kan man aldrig vara tillräckligt säker då digitaliseringen hela tiden utvecklas och chans för hackning blivit allt större än den var förr.

GDPR eller EU:s dataskyddsförordningen har börjat sätta sig ganska bra in hos ämbetsverk och förordningen ändras inte så hemskt mycket varje år vilket gör att ämbetsverk i lugn och

ro kan anpassa sig till de ändringar som kommer och hinner lära ut informationen till sina anställda. Dock måste förordningen gå framåt hela tiden så att den inte föråldras och eftersom den digitala världen går framåt hela tiden är ytterst viktigt att förordningen inte blir efter.

Utifrån intervjun lärde jag mig att ämbetsverk ypperligt försöker lära ut så mycket som de bara kan och vill att deras personal är medveten om de regler som gäller just behandling av andras personuppgifter. Utlärningen av dataskydd och GDPR är väldigt viktigt eftersom förebygger att uppgifterna används fel och minskar chanserna för sanktionsavgifter.

Med åren så har digitaliseringen blivit en allt större del i arbetslivet och hos företag och organisationer som sköter personuppgifter har man upptäckt att det ibland kan vara svårt att se till att allting går rätt till. Det är ganska lätt hänt att det uppstår något slags virus eller liknande dataläcka. Här kan man dock se att ämbetsverk tar dataskyddet på högsta allvar, de skickar ut sina e-mail via en säker server och alla mejl är låsta om det skickas från organisationens egna system, på intervjun tog jag och frågade Tullens dataskyddsanvsarig hur de går till väga då de skall skicka säkra e-mails som innehåller känslig information och då fick jag reda på att de använder sig just av ett system där de kan skicka ut säkrade email som endast går att öppna på en server och att meddelandet endast är giltigt i 30-60 dagar beroende på vad informationen gäller, i det vanliga fallet är det 30 dagar som gäller.

Men varför förnyades dataskyddslagen och varför togs den gamla lagen bort? I detta arbete undersökte jag hur ämbetsverk anpassat sig till den nya lagen och från detta arbete kan jag dra den slutsatsen att EU:s dataskyddsförordning gjordes för att göra det lättare då det gäller behandling av personuppgifter utifrån ett internationellt perspektiv, nu då alla medlemsländer har gemensamma riktlinjer och samma principer att följa blir det lättare att kontrollera att allting sköts på rätt sätt. På detta sätt kan EU kontrollera att de mesta går enligt lagen och att ingen utsätts för något olämpligt. Att tillägga här, utifrån min undersökning la jag märke till att dataskyddsförordningen gjorde det möjligt att samarbetet

mellan medlemsländerna ökade gällande behandling av personuppgifter eftersom de alla hade samma mål vilket är att trygga de registrerade och att hålla de registrerades information säker vilket också i praktiken har lyckats.

6 Sammanfattning

För att sammanfatta detta arbete så ändrade Dataskyddsförordningen inte så mycket på ämbetsverks verksamhet utan den mera förstärkte säkerheten och förordningen sågs mera som en förnyelse av den gamla personuppgiftslagen.

Hur har ämbetsverk påverkats av GDPR?

Ämbetsverk har påverkats mera administrativt än ekonomiskt och ämbetsverk har sett mer positivt än negativt på dataskyddsförordningen. Ända negativa var att det ännu inte finns hemskt mycket information gällande gemensamma regler med länder utanför EU eftersom dataskyddsförordningen endast tillämpar EU medlemsländer. Ämbetsverk har hamnat justera deras gamla verksamhetsplan lite grann gällande dataskydd men till det stora hela var den endast små justeringar då de redan från förr använt sig av en annan lag om personuppgifter.

Hur har förordningen påverkat arbetsprocessen?

Arbetsprocessen har ändrats på det sättet att fler säkerhetsåtgärder tillämpades på grund av dataskyddsförordningen, det lades till några extra resurser såsom dataskyddsanvsarig och dataskyddsombud. Ämbetsverken hamnade också forma in dataskyddet i deras processer då det gäller behandlingen av personuppgifter, deras personal måste ta kurser inom dataskydd och lära sig hur man skall hantera känslig information och andras uppgifter på ett professionellt sätt.

Vad fanns det för följder och risker om dataförordningen inte följs?

Följder och risker som följde dataskyddsförordningen är böter och skadeståndsansvar. Ämbetsverk måste följa de regler som står skrivna i dataskyddsförordningen, om inte så

hotas ämbetsverk med stora böter eller att de hamnar ersätta offret/offren som det gäller. Andra risker som från detta arbete kom synliga var att ämbetsverk gärna vill ha klarare verktyg då det gäller självaste arbetet.

För att ämbetsverk skall kunna hålla sitt rykte och hålla deras ord till deras kunder är det viktigt att de kommer ihåg att följa dataskyddsförordningens bestämmelser och inte gå utanför förordningens ramar eftersom det kan leda till stora följder.

Eftersom digitaliseringen går framåt hela tiden är det också viktigt för dataskydd och dataskyddsförordningen att göra det för att kunna stärka säkerheten på behandlingen av personuppgifter. Just nu är dataskyddsförordningen i bra skick men med en snabb utveckling i den digitala världen så får inte dataskyddsförordningen bli efter.

7 Litteraturförteckning

Wendleby, M., & Dag, W. (2019). *Dataskyddsförordningen GDPR- Förstå och tillämpa i praktiken.* Sanoma Utbildning.

Hur påverkar EU:s dataskyddsförordning (GDPR) företag och organisationer? (2022). Hämtat från Samlogic.com: https://www.samlogic.com/articles/gdpr-eu-dataskyddsforordningen-foretag-organisationer.htm

Europaparlamentets och rådets förordning (EU) 2016/679. (2022). Hämtat från https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=sv

Dataskyddslag. (2022). *Finlex.fi*. Hämtat från https://www.finlex.fi/sv/laki/alkup/2018/20181050

Datakollen.se. (2022). *Datakollen*. Hämtat från https://datakollen.se/vad-hander-om-bolag-och-organisationer-inte-foljer-gdpr/

Fagerström, N. (2022). Dataläckan från Vastaamo kan också leda till bedrägerier: "Det borde vara straffbart att använda personbeteckningar för att säkerställa vem en person är". *Svenska Yle*.

Studentens Digitalkompetens. (2022). Hämtat från Helsingfors Universitet: https://blogs.helsinki.fi/studentens-digitalkompetens/4-datasakerhet-och-dataskydd/4-2-hur-man-skyddar-sig-mot-hotfaktorer/datasakerhet-i-sociala-medier/

Backman, J. (2016). *Rapporter och Uppsatser.* Studentlitteratur.

Integritetskydds myndigheten. (2022). Hämtat från imy.se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/dataskyddsforordningen-i-fulltext/

Integritetsskyddsmyndigheten. (2022). Hämtat från Dataskydds förordningen: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/dataskyddsforordningen-i-fulltext/#A77

EU:s dataskyddsförordningen. (2022). Hämtat från https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/dataskyddsforordningen-i-fulltext/

Dataskyddsombudmannens byrå. (2022). Hämtat från Vilka rättigheter har den registrerade i olika situationer?: https://tietosuoja.fi/sv/vilka-rattigheter-har-den-registrerade-i-olika-situationer

Boverket. (2022). Hämtat från Riskbedöming i praktiken: https://www.boverket.se/sv/byggande/forebygg-fel-brister-skador/riskbedomning/riskbedomning-i-praktiken/

Finlex. (2022). Hämtat från Dataskyddslagen 1050/2018: https://www.finlex.fi/sv/laki/alkup/2018/20181050

Integritetsskyddsmyndigheten. (2022). Hämtat från De registrerades rättigheter: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/

Säkerhet. (2022). Hämtat från Integritetsskyddsmyndigheten: https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/tillaten-behandling--vilka-krav-galler/sakerhet/

Dataskydd. (2022). Hämtat från Dataombudsmannens byrå: https://tietosuoja.fi/sv/gdpr-sv

Känn till dina rättigheter. (2022). Hämtat från Dataombudsmannens byrå : https://tietosuoja.fi/sv/kann-till-dina-rattigheter

Dataskyddsombud. (2022). Hämtat från Dataskyddsombudsmannens byrå: https://tietosuoja.fi/sv/dataskyddsombud

Bildkällor:

Figur 1: https://blogs.helsinki.fi/studentens-digitalkompetens/4-datasakerhet-och-dataskydd/4-1-introduktion-till-datasakerhet-och-dataskydd/individens-dataskydd/

Figur 2: https://solatum.se/gdpr/

Figur 3: https://www.samlogic.com/articles/gdpr-eu-dataskyddsforordningen-foretag-organisationer.htm

Figur 5: https://www.boverket.se/sv/byggande/forebygg-fel-brister-skador/riskbedomning/riskbedomning-i-praktiken/

Figur 8: https://gdprcert.se/avsnitt/4-ansvar-och-roller/