YRKESHÖGSKOLAN
NOVIA

# Tillämpning av GDPR inom Erikssons-koncernen

## En implementering av GDPR inom ett företag i praktiken

Johan Sundqvist

Examensarbete för Ingenjörsexamen (YH)-examen

Utbildningen i Produktionsekonomi

Vasa 2019

**EXAMENSARBETE**

Författare: Johan Sundqvist

Utbildning och ort: Produktionsekonomi, Vasa Inriktningsalternativ/Fördjupning:

Handledare: Roger Nylund

Titel: Tillämpning av GDPR inom Erikssons-koncernen

---

Datum 03.05.2019Sidantal 30 Bilagor 3

---

**Abstrakt**

GDPR är en dataskyddsförordning som trädde i kraft den 25 maj 2018 och förkortningen står för General Data Protection Regulation. Detta ersätter EU:s dataskyddsdirektiv från år 1995.
Dess syfte definieras som att delvist få en harmonisering mellan Europeiska Unionens (Eus) medlemsstater samtidigt som det vill leda till en förstärkning av integritetsskydd et för fysiska personer inom EU-området. Dataskyddsförordningen omfattar endast EUmedborgare så folk bosatta utanför EU påverkas inte av GDPR.

I praktiken innebär en implementering av GDPR hos ett företag att kraven på att informera hur de hanterar uppgifter, vilka uppgifter och varför blir stärkta.

Företaget Erikssons behöver hjälp med att skapa ett regelverk med rutiner och med att göra en riskbedömning för att enkelt kunna förstå och tillämpa GDPR i praktiken. Syftet blir alltså att kunna förstå GDPR så bra som möjligt angående hur denna förordning ska tillämpas samt hjälpa Erikssons att kunna tillämpa denna förordning på ett lättförståeligt sätt.

---

Språk: Svenska Nyckelord: GDPR, personuppgift, personuppgiftsansvarig

---

**BACHELOR'S THESIS**

Author: Johan Sundqvist
Degree Programme: Environmental Engineering Specialization:
Supervisor(s): Roger Nylund

Title: An appliance of the GDPR for Erikssons

---

Date 03.05.2019 Number of pages 30 Appendices 3

---

GDPR is a data regulation taken into use on the 25th of May 2018 and its shortening stands for General Data Protection Regulation. This regulation replaces the data protection directive from the year 1995.
The purpose of the regulation is defined as to partly have a harmonization between the states within the EU and simultaneously it strives to strengthen the protection of integrity for physical persons inside the EU. The data regulation only applies in states within the EU which means that people living outside of it are not affected by the regulation.

Practically the implementation of the GDPR in an organization requires that they can inform how they are dealing with personal data, what data exactly and the purpose of dealing with it.

The Erikssons company has ordered me to create a framework containing routines for how to deal with personal data according to the GDPR and to also conduct a risk assessment to be able to easily understand and implement the GDPR in practice. The purpose of this thesis is to understand the GDPR as well as possible concerning how this regulation will be applied and to help Erikssons with applying it in an easily understandable way.

---

Language: Swedish Key words: GDPR, personal data, controller

---

# Innehållsförteckning

# 1 Inledning

GDPR, eller dataskyddsförordningen togs i bruk den 25:e maj 2018 och ersätter dataskyddsdirektivet från 1995. Orsaken till att GDPR ersätter detta dataskyddsdirektiv är för att det är föråldrat och blir mera irrelevant desto mer tiden går. Av denna orsak kan EU inte längre garantera säkerheten hos sina medborgare med hjälp av detta dataskyddsdirektiv. GDPR är en av EU:s förordningar och gäller därför bara för företag inom EU och de företag utanför EU som behandlar personuppgifter tillhörande EU-medborgare.

Detta arbete går ut på att utarbeta ett dokument med rutiner för Erikssons-koncernen så att de enklare ska kunna tillämpa GDPR-lagstiftningen och kunna förstå den enklare. Tillika ska jag också utföra en riskbedömning angående personuppgiftsbehandling som Erikssons kommer att kunna använda som ett verktyg för riskbedömningar i framtiden samt avslutningsvis en intervju med två personuppgiftsansvariga som är anställda av organisationen för att få en tydligare bild av hur företag har påverkats av GDPR i praktiken. Detta arbete kommer alltså att ge bra information om hur företag som behandlar personuppgifter påverkas av GDPR och vilka åtgärder som kan vidtas för att kunna tillämpa detta i praktiken.

## 1.1 Frågeställning

Frågeställningen för detta examensarbete är att kunna förstå hur ett företag som behandlar personuppgifter påverkas av dataskyddsförordningen och utifrån det kunna hjälpa företaget Erikssons med att komma med förbättringar för hur de ska kunna tillämpa den bättre. GDPR ger inga konkreta exempel på hur ett företag bör tillämpa förordningen så mycket lämnas till egen tolkning. Då återstår frågan vilket tillvägagångssätt bör tillämpas för att kunna göra detta, och svaret är att utarbeta rutiner och utföra en riskbedömning samt utföra en intervju för att få en bättre förståelse i hur GDPR i praktiken tillämpas.

## 1.2 Syfte och mål

Syftet med detta arbete är att göra det enklare för Erikssons att vidareanpassa sig till det nya regelverket GDPR. Detta genom att klargöra vad som bör tillämpas på företaget genom att skapa en lista med rutiner som företaget ska följa vid behandling av personuppgifter samt att jag vill få en förståelse över hur dataskyddsförordningen har påverkat verksamheten för de

företag som behandlar personuppgifter. Listan bör innehålla så mycket information som möjligt samtidigt som den är lätt att förstå.

Utöver dessa rutiner som bör finnas för att kunna tillämpa GDPR i praktiken utarbetas också rutiner på vad som bör göras när ett misstag, som en personuppgiftsincident har inträffat samt även utarbeta en modell för riskkartläggning för att enklare kunna förstå och förhindra risker som tillkommer när man behandlar personuppgifter.

Målet med detta arbete blir alltså att kunna förstå tillämpningen av GDPR så bra som möjligt för mig själv och för Erikssons och utarbeta det tidigare nämnda regelverket. Detta dokument ska ta upp utrymme på ett par A4-sidor och vara så enkel att förstå som möjligt samtidigt som de punkter som finns i nämnda dokument beskriver tillräckligt ingående och lättförståeligt hur kunders personuppgifter får behandlas.

## 1.3 Avgränsning

Mitt arbete utförs åt företaget Eriksson eftersom jag har arbetat åt dem under fyra somrars tid (2015-2018) och kommer att fortsätta ännu under 2019. Det känns därför rätt för mig att utföra detta arbete åt dem då jag under denna tid fått en bra insikt i företaget och dess verksamhet. En del av den info jag har att utgå ifrån är den jag har fått ta del av främst från skolningar som företagets personal deltagit i.

## 1.4 Struktur

I kapitel 2 och 2.1 beskrivs det vad Erikssons-koncernen är och vad den gör för att introducera läsaren till företaget och ge en bild över hur GDPR kan tänkas påverka detta företag. Det viktiga med det kapitlet är att förstå hur Erikssons är i behov av att kunna hantera sina kunders personuppgifter och hurudant kundförhållande det ger företaget.

I kapitel 3 går jag in på vad GDPR är och vad denna dataskyddsförordning är till för. Dess syfte är alltså att stärka integriteten hos fysiska levande personer. Här nämns den största skillnaden för hur företag härefter får behandla personuppgifter, nämligen inte utan samtycke eller anledning. I detta kapitel tar jag också upp om de sanktioner som kan tillfalla de organisationer som inte följer förordningen.

Annat som tas upp under tredje kapitlets underrubriker är vad personuppgifter är och hur de behandlas, samtycke, de registrerades rättigheter samt personuppgiftsansvarige och

personuppgiftsbiträde. Dessa delar beskriver var för sig vad man bör tänka på härefter när man behandlar personuppgifter och erhåller samtycke till behandling av dessa samt vem som är ansvarig för deras behandling.

Kapitel 4 ger sig in på hur GDPR tillämpas inom företag gällande personuppgiftesbehandling, säkerhet, risker samt vilka handlingar som en organisation bör utföra för att kunna fullgöra sina skyldigheter inom dataskyddsförordningen. I kapitel 4.2 om konkreta handlingar hänvisas mycket av det som jag utarbetat åt Erikssons och i kapitlen 4.2.4 och 4.2.5 ges grunden för riskbedömningen.

# 2 Erikssons

Företaget Erikssons grundades 1959 av Stig Erikssons, då som en verkstad i Esse som specialiserade sig på traktorer och bilar. Under decenniernas lopp har företaget utvecklats och består idag av fyra koncerner: Bildelsåtervinningen, Verkstaden, Bärgning och Transport och Skog och Trädgård. Den sistnämnda är en butik i Jakobstad som både säljer och erbjuder service av bl.a. motorsågar och gräsklippare. (Eriksson, u.d.)

Detta företag påverkas alltså av GDPR eftersom de samlar in personuppgifter av sina kunder och bör därför anpassa sig till de krav som ställs av GDPR. Dessa personuppgifter lagras i ERP-systemet DL Prime. Programmet DL Prime är i detta fall ett personuppgiftsbiträde, en viktig roll vad gäller hantering av personuppgifter som vi går igenom senare i detta arbete.

## 2.1 Verksamhet

Erikssons-koncernen består av fyra olika företag. Bildelsåtervinningen, som namnet säger, återanvänder delar från begagnade bilar. Detta betyder att företaget införskaffar begagnade eller oanvändbara fordon och går därefter igenom och ser vilka delar i dessa som lönar sig att restaurera upp och sälja vidare. Denna koncern har ett lager i vilket man via deras hemsida kan söka upp den del eller de delar som eventuellt kan finnas där.

Verkstaden erbjuder reparationstjänster på fordon samt lackering. Tillsammans med bildelsåtervinningen och bilbärgningen erbjuds alltså en heltäckande service för reparation av skadat fordon.

Bilbärgningen erbjuder tjänst dygnet runt för bärgning av fordon till en verkstad kunden själv väljer. Denna verksamhet har sitt hemområde i Jakobstad-Karlebynejden.

Det sista företaget i Erikssons-koncernen är Skog och Trädgård i Jakobstad. Här erbjuds försäljning av bl.a. motorsågar, gräsklippare, lövblåsare, robotgräsklippare, skyddsutrustning med mera samt service av dessa. Vad gäller robotgräsklipparna så erbjuds också frakt och installation av dessa. (Erikssons, u.d.)

# 3 Vad är GDPR?

GDPR, eller General Data Protection Regulation kallas det nya direktivet som EU tog i bruk 25 maj 2018. Detta nya direktiv strävar till att stärka EU-medborgares rättigheter. Eftersom mycket har ändrats sedan dataskyddsdirektivet togs i bruk 1995 så krävs ett uppdaterat och modernare direktiv för hur man får hantera personuppgifter.

GDPR innehåller alltså mycket som redan fanns i dataskyddsdirektivet, men det har även tillkommit flera bestämmelser. En annan skillnad är att dataskyddsdirektivet från 1995 är som namnet antyder, ett direktiv medan dataskyddsförordningen är en förordning. Skillnaden på dessa två är att ett direktiv ger utrymme för tolkning av hur ett land bör uppnå sina mål. En förordning däremot är bindande. Detta gör det självklart att ett större ansvar sätts på alla som behandlar personuppgifter.

Syftet med GDPR är att stärka skyddet för fysiska, levande personer. Det gäller alltså inte för företag, föreningar eller dylikt utan endast för människor. En av de viktigaste punkterna inom GDPR är att det inte längre är möjligt för företag att behandla fysiska personers personuppgifter utan samtycke eller anledning.

Ifall förordningen bryts mot kommer åtgärder att vidtas mot det företag, den myndighet eller annan juridisk person som begår brottet. En sådan åtgärd är en sanktion med bötfällning på upp till 4% av ett företags globala omsättning under föregående bokföringsår, eller på upp till 20 miljoner euro (€). Vilken av dessa man utgår ifrån vid en eventuell sanktion beror på vilket värde som blir högst. Under hot om sådana sanktioner strävar företag som lyder under GDPR naturligtvis till att ta detta på största allvar. (Wendleby, Wetterberg 2018, 11-26)

## 3.1 Personuppgifter

Vad är då en personuppgift? Med personuppgift avses sådana uppgifter som syftar på en identifierad eller identifierbar fysisk person, endera enskilt eller tillsammans med andra uppgifter. En identifierbar person kan vara endera direkt eller indirekt identifierbar. Detta

begrepp är brett och kan formuleras med hjälp av text, bild eller ljud. Sådana personuppgifter som ensamma kan användas för att identifiera en fysisk person kan vara personnummer, medan de som tillsammans med andra personuppgifter kan vara adresser eller förnamn. Eftersom GDPR endast innehåller information om hantering av personuppgifter är det viktigt att kunna definiera vad som menas med personuppgifter. (Wendleby, Wetterberg 2018, 3536)

Juridiska personer påverkas inte av GDPR, utan endast behandling av personuppgifter tillhörande fysiska, levande personer faller under förordningen. Det är dock viktigt att tänka på att innehavaren av ett företag alltid är en fysisk person. GDPR innefattar heller inte avlidna personer eller personer som inte ännu är födda. Det finns däremot släktingar till avlidna eller ännu inte födda personer (t.ex. vem som blir förälder) som omfattas av förordningen. (Wendleby, Wetterberg 2018, 38)

Det finns sådana personuppgifter som kallas för ”känsliga personuppgifter”. Huvudregeln med känsliga personuppgifter är att de inte är tillåtna att hantera. Känsliga personuppgifter syftar på t.ex. etniskt ursprung, religiös eller filosofisk övertygelse, politiska åsikter med mera. Sådana uppgifter anses som privata och kan i värsta fall leda till allvarlig diskriminering om de behandlas fel. Det enda fallet där sådana personuppgifter får behandlas är om den registrerade ger sitt samtycke till detta. (Wendleby, Wetterberg 2018, 41)

### 3.1.1 Personuppgifternas behandling

Det är vid behandling av personuppgifter som dataskyddsförordningen blir tillämplig. Begreppet ”behandling” är väldigt brett eftersom det avser all sorts användning av personuppgifter. Det innefattar läsning, ändring, spridning, lagring, radering och förstörande av dem.

Dataskyddsförordningen säger att all behandling av personuppgifter bör vila på en laglig grund. Följande lagliga grunder, endera ensamma eller tillsammans med andra måste uppfyllas innan behandling är tillåten:

- Den registrerade har lämnat sitt samtycke för att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

- Behandlingen bör vara nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett avtal ingås.

- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person.
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

(Wendleby, Wetterberg 2018, 43-45)

Det finns dock ett undantag i när behandling av personuppgifter inte faller inom dataskyddsförordningen. Det är när behandling av personuppgifter sker inom rent personligt bruk eller sker inom verksamhet som inte omfattas av GDPR. Det kan då röra sig om försvar eller nationell säkerhet och personuppgiftsbehandling som strävar till brottsbekämpning, som polisens arbete. (Wendleby, Wetterberg 2018, 54)

Utöver att det finns ett grundläggande krav på att behandling av personuppgifter måste ske på ett lagligt sätt så finns också övriga principer för behandling av dessa. Den viktigaste principen är att personuppgifter ska behandlas på ett lagligt, öppet och korrekt sätt. Också att tänka på är att uppgifter bara får användas för de ändamål som de är insamlade för, dvs. att när en kund ger sitt samtycke så begränsas användningen till endast de specificerade syften som bör ha nämnts och godkänts. (Wendleby, Wetterberg 2018, 49-50)

### 3.1.2 Samtycke

En viktig punkt som tillkom med GDPR är att vid insamlingen av personuppgifter bör man tänka på de kravs som ställs på samtycket. Samtycke bör vara frivilligt och ges genom ett uttalande eller bekräftande handling och bör ges efter att den registrerade har fått information om personuppgiftsbehandlingen.

Den som behandlar personuppgifter (personuppgiftsansvarige) bör kunna ge bevis på att ett giltigt samtycke getts av den registrerade. En sammanfattning är att samtycke innebär att den

registrerade själv har uttryckt ett medgivande till viss behandling av dennes personuppgifter. (Datainspektionen, u.d.)

### 3.1.3 Personuppgiftsansvarige och personuppgiftsbiträde

Personuppgiftsansvarig är den person, endera juridisk eller fysisk, offentliga myndighet, institution eller annat organ som bestämmer syftena och metoderna för personuppgiftsbehandlingar. (GDPR, 2016, 112)

Två eller flera företag kan ha ett gemensamt ansvar och då fastställer alla parter ändamålen och medlen för behandlingen. De gemensamt personuppgiftsansvariga ska fastställa sitt respektive ansvar för att fullgöra sina skyldigheter. (Frydlinger, Edvardsson, Olstedt Carlström, Beyer 2018, 55)

De företag som bestämmer ändamål, syfte och metoder, alltså hur och varför de behandlas, faller alltså inom ramen för EU:s regelverk. Flera skyldigheter kommer med detta personuppgiftsansvar. De personuppgiftsansvariga är skyldiga att meddela personuppgiftsincidenter till tillsynsmyndigheten. (Wendleby, Wetterberg 2018, 28-29)

Personuppgiftsbiträde är en extern part som får ta del av organisationens personuppgifter eftersom de utför tjänster som innefattar behandlingar av personuppgifter.
Personuppgiftsbiträde kan vara en fysisk eller juridisk person och bör kunna ge tillräckliga garantier för att behandlingen uppfyller de krav som ställs av dataskyddsförordningen. Ett personuppgiftsbiträde har inte rätt att anlita en annan part för att behandla personuppgiftsansvariges personuppgifter utan tillåtelse av personuppgiftsansvarige. (GDPR, 2016, 112) (Wendleby, Wetterberg 2018, 106-107)

Förhållandet fungerar så att personuppgiftsansvarige som ger instruktioner om hur personuppgiftsbiträde får behandla personuppgifter och personuppgiftsbiträdet får enbart behandla personuppgifterna i enlighet med dessa instruktioner. De instruktioner som lämnas bör naturligtvis följa regleringarna i dataskyddsförordningen. (Frydlinger, Edvardsson, Olstedt Carlström, Beyer 2018, 56-57)

### 3.1.4 Personuppgiftsbehandling i E-post

Vid användning av E-post så gäller det i princip att man behandlar personuppgifter med tanke på att en E-postadress är en personuppgift. Vid behandling av personuppgifter i e-post

krävs en rättslig grund för behandling. Behandling av personuppgifter i e-post är bristfälligt med tanke på säkerheten eftersom innehållet sällan är känt när det når verksamheten samt att denna typ av plattform inte har en hög säkerhetsnivå.

Långsiktig lagring av personuppgifter i e-post är inte ett rekommenderat sätt ur personuppgiftsbehandlingsperspektiv. Därför är det säkrare att flytta innehållet från e-posten så snabbt som möjligt till ett säkrare system.

Det som rekommenderas angående behandling av personuppgifter i e-post är att bedöma om uppgifterna ska bevaras och var för att uppfylla de krav som gäller dessa uppgifter, inte behandla känsliga personuppgifter i e-post, informera på organisationens hemsida hur personuppgifter i e-post behandlas, om man skickar svarsmejl bör man bifoga en standardtext innehållande information om hur personuppgifter behandlas och skicka information till organisationens alla verksamma angående regler och rutiner för hur man behandlar personuppgifter. (Datainspektionen, u.d.)

## 3.2 Den registrerades rättigheter

I dataskyddsförordningen bestäms att den registrerade ska förstärkt rätt till information och uppgifter jämfört med tidigare. En registrerad definieras som en fysisk person som åtnjuter skydd för sin integritet under dataskyddsförordningen. Den registrerade är en identifierad eller identifierbar fysisk person vilket utesluter juridiska personer från detta skydd. (Frydlinger, Edvardsson, Olstedt, Beyer 2018, 57-58)

Sammantaget innebär detta en förstärkning av den enskildes personliga integritet. Den registrerade har härefter

- Rätt till information som innebär att den registrerade har rätt att få vetskap om behandlingar när dennes personuppgifter behandlas. Den information som den registrerade får ska innehålla vilken typ av behandling som gjorts.

- Rätt till tillgång, detta innebär att den registrerade har rätt att få bekräftelse på att denna behandlats av organisationen, vilket kan vara en historik angående behandlingarna. Om information begärs så ska organisationen kunna lämna ut detta till den registrerade utan att dröja, senast en månad efter att det tillfrågats.

- Rätt till rättelse tillämpas när den registrerades personuppgifter är felaktiga. Den registrerade har också rätten att komplettera sina personuppgifter ifall relevant information saknas. När information om personuppgifter rättats har organisationen skyldighet att meddela alla registrerade som berörs att rättelse har blivit utförd.

- Rätt till radering som namnet innebär är den registrerades rätt att kunna få sina personuppgifter raderade. Radering av personuppgifter bör kunna göras ifall personuppgifterna inte längre behövs, ifall behandlingen grundar sig på samtycke och den registrerade återkallar samtycket, om den registrerade motsätter sig behandling av dennes personuppgifter i direktmarknadsföringssyfte, ifall den registrerades intressen väger tyngre än organisationens efter en intresseavvägning, vid olaglig behandling av personuppgifter, om det är en rättslig skyldighet att radera personuppgifterna och om behandlingen avser barn vars personuppgifter behandlats som ett led i tjänster av informationssamhället.

- Rätt till begränsning av behandling innebär att personuppgifter begränsas så att de bara får behandlas för vissa avgränsande syften. Detta kan krävas i kombination med rätten till rättelse som så att under tiden dennes personuppgifters korrekthet utreds är också behandlingen av personuppgifterna begränsade, bland andra möjliga situationer som kan uppstå i vilka de registrerade utkräver denna rätt.

- Dataportabilitet är till för om den registrerade behöver flytta över den lagrade informationen om sig själv till en annan plattform. Det är då organisationens skyldighet att kunna förenkla en flytt av information från sin egen datamiljö till en tredje parts. Denna rätt baserar sig dock på om hur avtalet har formulerats.

- Rätt till att göra invändningar tillämpas ifall den registrerade anser att rätten är befogad med hänvisning till dennes speciella situation mot organisationen ifall de lagliga grunderna i allmänt eller enskilt intresse. I detta fall läggs bevisbördan på organisationen. Denna rätt kan hänvisas till ifall personuppgifterna använts för profilering kopplad till direktmarknadsföring.

- Rätt till skydd mot automatiserat beslutsfattande. Den registrerade har rätt att inte bli föremål för denna typ av beslut ifall besluten kan ha rättsliga följder för denne eller på liknande sätt påverkar den enskilde i betydande grad.

Utförande av dessa bör kunna tillämpas endera vid behandling eller på begäran av den registrerade. Sådan information har organisationen skyldighet till att kunna ge lättillgängligt, utan kostnad och skrivet på lättförstått och tydligt språk till den registrerade. Detta bör också innehålla information angående vilken behandling som utförts av den personuppgiftsansvarige.

(Wendleby, Wetterberg 2018, 91-103)

Vad som krävs av en organisation är då att upprätta rutiner som på ett så enkelt sätt som möjligt gör att den kan kommunicera behandlingen av personuppgifter inom tidsramen som gäller i dataskyddsförordningen. Det är sådana rutiner som jag ska utarbeta åt Erikssons.

## 3.3 Personuppgiftsincidenter

En personuppgiftsincident är en händelse som innebär risker för en fysisk persons rättigheter och friheter. De risker som förekommer innebär bl.a. att den registrerade förlorar kontrollen över sina uppgifter eller att dennes rättigheter inskränks. Exempel på vad en personuppgiftsincident kan leda till är diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust och brott mot sekretess eller tystnadsplikt.

Det anses vara en personuppgiftsincident ifall personuppgifter har blivit förstörda, gått förlorade eller hamnat i orätta händer och det spelar ingen roll ifall det skett oavsiktligt eller avsiktligt för att det ska var en personuppgiftsincident.

Anmälningsskyldighet råder för vissa typer av personuppgiftsincidenter och denna skyldighet har en tidsfrist på 72 timmar. Den eller de registrerade som incidenten är riktad mot bör också informeras angående incidenten. (Datainspektionen, u.d.)

# 4 GDPR inom organisationer

För de företag som har ett kundregister så gäller GDPR-förordningen. Dataskyddsförordningen vill att organisationer ska sträva till att ständigt bli bättre på att stärka den enskildes integritet och förbättra dennes makt över sina egna personuppgifter. Detta innebär att nya utmaningar har tillkommit för sådana företag så de inte får behandla personuppgifter på samma sätt som de gjort tidigare.

För att ta sig an förordningen så finns det åtgärder att vidta. Dessa är

- Personuppgiftsansvariga bör genomföra lämpliga organisatoriska åtgärder, som att tillsätta ett dataskyddsombud med tillräcklig kompetens och resurser för arbetet, ta fram tydliga strategier och rutiner för dataskyddsarbetet, hålla personalen utbildad med mera.

- Den personuppgiftsansvariga ska genomföra lämpliga tekniska åtgärder. Dessa kan vara att säkra alla IT-system och se över olika säkerhetsåtgärder, men också kolla om organisationen kan erbjuda dataportabilitet.

- Personuppgiftsansvariga ska under alla omständigheter säkerställa att de grundläggande principerna för behandling iakttas.

- Organisationen ska i sina tekniska beslut väga in den dels senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål och riskerna för fysiska personers rättigheter och friheter för att ständigt förbättra sin tekniska och organisatoriska nivå.

(Wendleby, Wetterberg 2018, 151)

Som syns ovan så kan det vara väldigt utmanande för företag att ta sig an detta, speciellt med tanke på att kraven är så höga.

## 4.1 Villkor för samtycke

Dataskyddsförordningen har gjort villkoren tydligare vad gäller villkoren för samtycke. Det bör vara specifikt och informerat och utgöra ett otvetydigt medgivande från den registrerade parten. Något som medförs av detta är att man kunde ha den registrerade att välja vilka användningsområden den samtycker till, och vilka den väljer att lämna bort.

De användningsområden som kan tillämpas är:

- Att administrera kundförhållandet
- Marknadsföring
- Säkerhetsfrågor
- Reklam från andra samarbetspartners och andra koncernbolag
- Att lämna ut uppgifter till samarbetspartner

- Affärs- och metodutveckling

Tillika gäller andra krav på samtycket, t.ex. att den som gett samtycke när som helst ska ha rätt att återkalla det, och att detta informeras om. Även det att språket måste vara lättförstått, och om samtycket bör kunna särskiljas om det är inkluderat i ett mera ingående avtal.

(Wendleby, Wetterberg 2018, 51-53)

## 4.2 Konkreta handlingar

Vad ska då ett företag göra om man ser mera detaljerat på åtgärderna? Intern styrning och kontroll är viktigt här. Konkreta åtgärder man bör ta till är att inventera, ta i bruk ett register i vilket information om all personuppgiftsbehandling lagras, utse ett dataskyddsombud, vara måna om och i nödfall, kunna hantera risker och hantera säkerheten. Alla dessa går vi igenom till näst.

### 4.2.1 Inventering

Det är inom ett företag viktigt att förstå den egna organisationens funktioner för att kunna utveckla effektiva styrdokument och rutiner. Man kan göra detta genom att framställa en lista över de personuppgifter som finns. Denna lista byggs upp med hjälp av organisationens registerförteckning.

När man utfört en inventering blir det enklare för organisationen att övervaka att styrdokument och processer följs upp. En inventering bör hållas uppdaterad med tiden eftersom dess värde snabbt försvinner ifall denna handling försummas.

(Frydlinger, Edvardsson, Olstedt Carlström och Beyer 2018, 119-120)

### 4.2.2 Register

När personuppgifter behandlas så krävs av den personuppgiftsansvarige eller personuppgiftsbiträdet att för register över handlingar. Registret, som kan vara ett dokument, bör vara skriftligt, finnas tillgängligt i elektroniskt format och vara uppdaterat. Registret bör innehålla

- Den personuppgiftsansvariges namn och kontaktuppgifter
- Behandlingens ändamål

- En beskrivning av kategorierna av registrerade och personuppgifternas kategorier
- De kategorier av mottagare till vilka personuppgifterna endera har eller ska lämnas ut inbegripet mottagare i tredjeländer eller i internationella organisationer
- I tillämpliga fall överföringar av personuppgifter till tredjeland eller en internationell organisation
- De förutsedda tidsfristerna för radering av de olika kategorierna om möjligt
- En allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna.

Personuppgiftsbiträdet bör också ha ett register som innehåller följande punkter:

- Personuppgiftsbiträdets namn och kontaktuppgifter och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar
- De kategorier av behandling som utförs för den personuppgiftsansvariges räkning
- Överföringar av personuppgifter till tredjeland eller internationell organisation inbegripet identifiering av dessa, om tillämpligt
- En allmän beskrivning av tekniska och organisatoriska åtgärder om det är möjligt.

(Datainspektionen, u.d.)

### 4.2.3 Att utse dataskyddsombud

Tidigare i detta kapitel nämndes dataskyddsombud. Dess roll är att övervaka efterlevnaden av dataskyddsförordningen, informera och ge råd till personuppgiftsansvarige angående vilka skyldigheter som gäller enligt dataskyddsförordningen samt fungera som kontaktperson till datainspektionen. Dataskyddsombud ska utses på grund av sin kompetens och kunskap i lagstiftning och praxis kring dataskydd.

Dataskyddsombudet ska av personuppgiftsansvarige involveras tidigt i frågor vilka gäller för personuppgifter och bör ha tillräckliga resurser för att kunna utföra sina arbetsuppgifter. (Wendleby, Wetterberg 2018, 113-114)

En organisation bör enligt dataskyddsförordningen utse ett dataskyddsombud ifall personuppgiftsbehandlingen utförs av en myndighet eller ett offentligt organ. Dataskyddsombud utses även om den personuppgiftsansvariges eller

personuppgiftsbiträdets kärnverksamhet består av personuppgiftsbehandling som kräver regelbunden och systematisk övervakning av den registrerade i stor omfattning. Ett dataskyddsombud krävs dock endast vid företag som har över 250 anställda. (GDPR 2016, 170-171)

### 4.2.4 Säkerhet

Kraven på säkerhet har ökat med dataskyddsförordningen med beaktande av utveckling, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt risker. Detta för fysiska personers rättigheter och friheter och det är upp till den personuppgiftsansvarige och personuppgiftsbiträdet att ta till de åtgärder som krävs för att en lämplig säkerhetsnivå upprätthålls. Dessa åtgärder är:

- Pseudonymisering och kryptering. Pseudonymisering betyder att data behandlas utan att det är möjligt att identifiera en fysisk person. Kryptering kallas det när man gör information svårläsligt för den som inte är avsedd att ta del av den. Denna åtgärd fungerar bra vid behandling av information via E-post.
- Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna.
- Förmågan att återställa tillgängligheten och tillgången till personuppgifter inom en rimlig tid vid en fysisk eller teknisk incident.
- Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten för de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

(GDPR 2016, 160-161)

### 4.2.5 Risker och riskbedömning

Ett företag eller organisation är skyldigt att meddela den registrerade om risker med verksamhetens dataskydd. Det är ett krav att man går igenom och bedömer de risker som är förknippade med behandling av personuppgifter innan sådan behandling påbörjas.

Med en riskanalys kan man identifiera de åtgärder som man ska vidta för att hantera riskerna och kunna trygga en ändamålsenlig behandling av personuppgifter. Den

personuppgiftsansvarige bör också se till att dataskyddsprinciperna iakttas på ett så effektivt sätt som möjligt i förhållande till riskerna som är förknippade med behandlingen.

En riskbedömning är viktigt att se igenom, eftersom detta hjälper att se vilka åtgärder som är mest akuta. I en traditionell riskbedömning går organisationen själv igenom sina egna risker och bedömer dessa. När man utför en riskbedömning så går man igenom vilka hot, konsekvenser och åtgärder för att kunna minska riskerna.

I en riskbedömning bör flera olika perspektiv beaktas. Det viktigaste perspektivet som bör beaktas är om den registrerades rättigheter och friheter löper risk för att kränkas. Samtidigt ska den personuppgiftsansvarige också bedöma riskerna för sig själv och personuppgiftsbiträdet. Frågor som man kan tänka på när man utför en risk- och konsekvensbedömning beskrivs nedan:

- Finns stora problem med faktorer som kan leda till höga sanktionskostnader?
- Finns stora risker för den registrerade med behandlingen?
- Behöver konsekvensutredningar göras beträffande pågående behandlingar?
- Har dataskyddsincidenter inträffat?
- Saknas struktur som stöder GDPR?

(Wendleby, Wetterberg 2018, 246-248)

Jag har utarbetat en riskkartläggningstabell åt Eriksson eftersom de inte tidigare utfört en sådan vad gäller behandling av personuppgifter. Denna kartläggning innehåller riskbedömning, konsekvensbedömning samt en indikator som visar hur viktigt det är för organisationen att åtgärda problemet innan en eventuell incident inträffar. De punkter som nämns ovan kommer också att inkluderas i det dokument som överlämnas till Erikssons.

# 5 Mitt arbete åt Erikssons

Med den info som jag har fått ta del av ska jag i detta kapitel utarbeta de riktlinjer som tidigare nämndes, för att kunna förstå GDPR. Detta ska bli till ett eget dokument bestående av ett par eller några A-4 sidor. Innehållet bör vara så mångsidigt som möjligt samtidigt som det är lättförstått. Detta nämnda dokument lämnas in som separat bilaga vid sidan om detta

arbete. Innan detta ska vi ännu bekanta oss med de ERP-system som bör beaktas när jag bygger upp allt detta.

## 5.1 DL Prime

Erikssons använder sig av ERP-systemet DL Prime. Det är ”En heltäckande företagsprogramvara som omfattar allt från försäljning, ekonomiförvaltning och Logistik till CRM och webshop” enligt utvecklarnas hemsida. Servern, i vilken all information angående personuppgifter lagras, finns i Skog och Trädgård-butiken i Jakobstad. För Erikssons del så kan DL Prime ses som personuppgiftsbiträde

Detta program passar för både stora och mindre företag och omfattar 70 moduler som möjliggör det för att skräddarsys för företagets behov. Detta program lämpar sig också för löneadministration. Med andra ord är detta program i vilket Erikssons har sitt register med personuppgifter som jag är tvungen att utgå från när jag utarbetar riktlinjerna. (DL Software, u.d.)

## 5.2 Utarbetade rutiner

I detta kapitels genomgång tas det upp om vilka rutiner som utarbetats åt Erikssons och varför samt ges det en beskrivning av hur jag kom fram till de slutsatser som dras. Innan vi går igenom rutinerna så har jag skrivit in ett påpekande om att varje handling som gäller personuppgifter räknas som personuppgiftsbehandling, detta inkluderar passiv lagring. Detta presenteras i en lista som framställts nedan.

- Det första jag nämner är att varje personuppgiftsbehandling bör ske i enlighet med den rådande lagstiftningen. Väldigt självklart påpekande men som jag anser att är bra att ha som grund för personuppgiftsbehandling.

- Detta följs av personuppgiftsansvarige är skyldig att se till att dataskyddsförordningen följs. En person bör ha kontroll över situationen och detta ansvar faller naturligtvis på personuppgiftsansvarige.

- Som tredje rutin valde har jag skrivit att erhållande av samtycke bör kunna bevisas med tydliga regler för hur vi erhåller samtycke. Här nämns att samtycket bör ges entydigt och klart och i skriftlig form samt att detta bör dokumenteras. Med

hänvisning till dataskyddsförordningen skrev jag också att samtycke bör kunna dras tillbaka.

- Följande rutin handlar om syftet med personuppgiftsbehandlingen och att detta bör klargöras för den registrerade och att han eller hon ska ha möjlighet till att bara godkänna de delar som han eller hon är intresserad av. Som jag tidigare i detta arbete klargjort är att GDPR ger den registrerade möjlighet att få välja för vilka syften dennes personuppgifter får behandlas.

- Som femte rutin har jag skrivit att personuppgifter inte får behandlas i annat syfte än för det som man kommit överens om.

- Nästa rutin blir att föra register över behandlingen. Här har programmet DL en viktigare roll eftersom det erbjuder en sådan funktion. Ett register är obligatoriskt att ha vid behandling av personuppgifter med hänvisning till GDPR.

- Följande punkt är det påpekandet att tillgången till personuppgifterna ska bara tillåtas för de behöriga. Obehörig åtkomst är nämligen ett brott mot dataskyddsförordningen.

- Den åttonde rutinen är uppmanandet att hålla personuppgifterna korrekta och uppdaterade och att ifall förändring har inträffat för den registrerade så bör personuppgifterna också ändras.

- Nästa rutin handlar om radering av personuppgifter som inte längre behövs och radering på den registrerades begäran.

- Som tionde rutin har jag uppmanat att inte samla in mera personuppgifter än vad Erikssons behöver och om det har inträffat bör de överflödiga personuppgifterna omgående raderas.

- Den elfte rutinen handlar om säkerheten för den registrerade och här uppmanar jag till att förhindra personuppgifts- och dataskyddsincidenter och hänvisar till en senare del av dokumentet om vilka åtgärder som bör vidtas ifall sådana har inträffat.

- Som tolfte och därmed sista rutin har jag uppmanat Erikssons att tydliggöra rättigheterna för den registrerade. Jag har skrivit ett skilt kapitel i dokumentet som handlar om detta.

De rutiner som räknas upp följer varandra i den ordning som jag anser är viktigaste först. Den tolfte rutinen passar bra som avslutning eftersom följande kapitel i bilagan handlar om den registrerades rättigheter, alltså följs denna rutin med detsamma upp av relaterat material.

## 5.3 Ifall något går fel

I detta kapitel går jag igenom vad som bör göras vid Erikssons ifall olyckan är framme, dvs. ifall t.ex. en personuppgiftsincident inträffar. Jag anser att det är viktigt att ha detta som en rutin eftersom om just en personuppgiftsincident inträffar så kan det leda till allvarliga följder främst för den registrerade men också för företaget.

Vad Erikssons bör ha som rutin har jag i det dokument som jag utarbetat åt företaget lagt som ett eget kapitel. Även dessa rutiner presenteras i punktform och är också här placerade enligt ordningen viktigaste först.

- Som första punkt i detta kapitel är uppmaningen om att meddela dataskyddsmyndigheten inom 72 timmar när en personuppgiftsincident inträffat. Detta har jag skrivit av den orsaken att det är en kränkning av förordningen att inte meddela, vilket kan leda till grova sanktioner mot företaget samt allvarliga följder för de registrerade.

- Som andra rutin har jag skrivit att företaget bör meddela den registrerade angående personuppgiftsincidenten ifall denna innebär risker för honom eller henne. Här har jag också skrivit in att vi ger informationen klart och tydligt angående incidentens art och vilken kontaktpunkt den registrerade bör kontakta för mera information, enligt anvisningar från dataskyddsförordningen. Detta innebär också att man bör meddela om sannolika konsekvenser och vilka åtgärder Erikssons vidtagit för att åtgärda incidenten samt att det hör till att man ger rekommendationer angående vilka säkerhetsåtgärder den registrerade kan vidta för att mildra de negativa effekterna.

- Som tredje rutin skrev jag att Erikssons bör meddela personuppgiftsbiträdet DLorganisationen angående en dataskyddsincident eftersom de begärt att kunden ska göra så, detta för att DL ska kunna kartlägga de risker som deras mjukvara kan råka ut för.

- Den fjärde rutinen är uppmaningen om att dokumentera alla personuppgiftsincidenter och vad som bör ingå i denna dokumentation, dvs. incidentens omständigheter, dess

effekter, korrigerande åtgärder som vidtagits. Detta med förklaringen att dataskyddsmyndigheten ska kunna uppfölja att företaget efterlever dataskyddsförordningen.

- Följande rutin är att företaget ska anteckna alla kontakter och råd som företaget får från dataskyddsmyndigheten. Detta är egentligen inte en obligation utan snarare en rekommendation som är värd att följa.

- Till näst är påpekandet att om en anmälan görs senare än 72 timmar från det att en personuppgiftsincident har upptäckts så krävs det att man kan ge en orsak till varför förseningen inträffat.

- Som sista rutin i kapitlet ”Om något går fel” är att ifall personuppgiftsbiträdet (DL) råkar ut för en incident så bör det meddelas åt Erikssons för att företaget ska kunna fullgöra sina skyldigheter. Detta som sista rutin eftersom det i slutändan är en rutin som står utanför Erikssons makt och därför helt tillfaller DL-organisationen.

## 5.4 Riskkartläggning

Eftersom det är nödvändigt att kunna identifiera de risker och konsekvenser som tillkommer med personuppgiftsbehandlingar tog jag beslut med Erikssons om att göra en riskkartläggning. Denna riskkartläggning innehåller möjliga risker och vilka konsekvenser de medför samt vilka åtgärder som vidtas för att förhindra dessa, eller för hur vi hanterar dem om de uppstår.

DL-organisationen har i sin roll som personuppgiftsbiträde beaktat de risker som tillkommer för mjukvaran men flera av de riskerna är också relevanta för Erikssons-koncernen och därför spelar DL Prime en viktig roll i denna kartläggning.

Vid en riskbedömning är det värt att tänka på att det inte finns några givna värden på t.ex. hur en viss konsekvens ska bedömas, utan detta lämnas helt till den egna verksamheten att kunna fastställa.

Riskkartläggningen är utarbetad i programmet Microsoft Excel och fungerar som så att man bedömer risken med värdet 1-5 samt konsekvensen av om en viss handling misslyckas med samma värden, 1-5. Därefter multipliceras dessa värden med varandra och den ruta i vilken produkten av dessa värden räknas ihop i får en färg. Dessa färger är grön, gul och röd. Färgen

grön berättar att inga eller endast små åtgärder bör vidtas för att åtgärda risken, medan färgen gul berättar att medelstora åtgärder krävs och slutligen berättar den röda färgen att stora åtgärder omedelbart krävs för att åtgärda risken innan något går fel.

| Röd | Gul | Grön |
|---|---|---|
| Stora anpassningar behövs omedelbart. | Stora eller medelstora anpassningar behövs. | Ingen, eller endast mindre anpassningar behövs. |

**Sammanfattning av vad färgerna betyder.**

De frågor som ställs i riskbedömningstabellen är frågor som generellt kan tänkas uppstå hos ett företag som hanterar personuppgifter, alltså inga frågor som identifierats direkt hos Erikssons. Ett företag ska i huvudsak själva gå igenom och ta reda på angående och identifiera potentiella risker.

En tom mall lämnas därför in åt företaget eftersom det i framtiden finns behov av att kunna bedöma risker och dess konsekvenser varefter de identifieras eftersom en riskbedömning inte är något man bör göra bara en gång, utan är en handling som bör utföras regelbundet. Den personal som berörs av detta har blivit instruerade i hur denna modell för riskbedömning används och kan därför själva i fortsättningen själva hantera en riskbedömning.

Den riskbedömningstabell som jag lämnar in åt Erikssons är en förbättring på den som används i den riskbedömning som jag var med och utförde. Förbättringen är att den tomma tabellen har ett bredare textfält för att kunna skriva ut den i pappersform. Detta för att den delvis ska gå enklare att använda digitalt men framför allt att den ska bli praktisk i pappersform med tillräckligt mycket utrymme för att också kunna skriva in möjliga åtgärder.

| Identifierad risk + möjlig åtgärd | Sannolikhet | Konsekvens | Riskfaktor |
|---|---|---|---|
| | 1-5 | 1-5 | 1-25 |
| | | | **0** |
| | | | **0** |

**Exempel på riskbedömningstabellen som jag framställt i Excel.**

| Risker | Sannolikhet | Konsekvens | Risk |
|---|---|---|---|
| | 1-5 | 1-5 | 1-25 |
| Vad är risknivån för att en dataskyddsincident inträffar? | 1 | 3 | **3** |
| Hur är situationen med dataskyddsombud? | 1 | 1 | **1** |
| Finns risk för obehörig åtkomst till programmet? | 3 | 3 | **9** |
| Risk för Ransomware eller doxware? | 2 | 3 | **6** |
| Kan vi hantera en personuppgiftsincident? | 2 | 4 | **8** |
| Finns integritetsrisker med vår personuppgiftsbehandling? | 1 | 3 | **3** |
| Riskerna med vårt dataskydd? | 1 | 3 | **3** |
| Pseudonymisering och kryptering? | 3 | 3 | **9** |
| Förmågan att återställa tillgång och tillgänglighet till personuppgifter? | 1 | 3 | **3** |
| Riskfaktor för tester av säkerheten? | 2 | 3 | **6** |

**Riskbedömningstabellen efter att riskbedömningen utförts.**

### 5.4.1 Förebyggande åtgärder för de identifierade riskerna

Som det syns i riskbedömningstabellen så stöter inte Erikssons på några risker som kräver omedelbara och stora åtgärder. Några har dock hamnat på färgen gul vilket innebär att medelstora anpassningar krävs för att åtgärda de möjliga riskerna.

Den första frågan som fick färgen gul är ”Finns risk för obehörig åtkomst till programmet?”. Denna risk ansågs högre eftersom personalen sällan loggar ut från de datorer i vilka DL används för att hantera personuppgifter. En möjlig konsekvens av detta vore alltså att personuppgifter kunde hamna i fel händer eller avsiktligt förstöras. En föreslagen åtgärd är att den personal som använder sig av dessa datorer börjar logga ut från datorerna när de inte används, detta inkluderar när arbetsdagen avslutas.

Den andra frågan som fick gul färg handlar om risken för ransomware eller doxware. Motiveringen är att det alltid finns risk för att ett sådant program ska kunna ta sig in i datorn och förstöra. En åtgärd är att begränsa E-postanvändningen, eller rent av minimera den och bara öppna meddelanden från betrodda avsändare.

Tredje frågan som fick gul färg är om Erikssons kan hantera en personuppgiftsincident. Begreppet personuppgiftsincident är väldigt brett så det är svårt att beakta allt som kan inträffa. Värdet på konsekvensfaktorn blev därför 4 i kombination med hur allvarliga konsekvenser som kan uppstå ifall personuppgiftsincidenter inte kan hanteras. Åtgärder som föreslogs är att fortsätta att utföra riskbedömningar för att kunna identifiera risker innan de inträffar, följa rutiner som utarbetats för hantering av personuppgiftsincidenter och tillsätta en grupp och utarbeta en handlingsplan för hantering av personuppgiftsincidenter.

Fjärde frågan som har gul färg är angående pseudonymisering och kryptering. Erikssons använder sig sällan av dessa metoder för säkerhet och därför är den föreslagna åtgärden att utarbeta ett system för hur verksamheten oftare ska använda sig av detta så att inte information hamnar i fel händer.

Den sista frågan i denna riskbedömning är angående hur tillförlitligt testerna av säkerheten är. Testerna själva bedöms vara tillförlitliga men utförs sällan. Den självklara åtgärden i detta fall blir alltså att utföra tester på säkerheten mera regelbundet.

Slutligen går vi också igenom de risker som fått grön färg och ger motivering till varför de bedömdes som de gjorde.

Första frågan som fått grön färg handlar om det finns risk för att Erikssons drabbas av en dataskyddsincident. Risknivån är på 1 av den orsaken att man ansåg att dataskyddet är tillräckligt stark och programmet DL har beaktat flera risker som kan uppkomma hos programmet att det inte finns orsak till oro angående dataskyddsincidenter.

Frågan angående dataskyddsombud har båda faktorerna på 1 med motiveringen att företaget självt känner till hur man bör agera i sådana frågor som rör detta. Detta inkluderar att kontakta dataskyddsmyndigheten ifall en incident inträffar.

Inget antyder på att det skulle finnas integritetsrisker med den personuppgiftsbehandling som sker hos Erikssons för den registrerade eftersom man har kännedom i hur personuppgifter hanteras korrekt och att de endast behandlas för det syfte som de är ämnade för.

Angående frågan om det finns risker för Erikssons dataskydd så är risken också låg eftersom det skydd och de skyddsåtgärder som vidtagits anses tillräckliga.

Den sista frågan som inte kräver nya åtgärder är den om Erikssons förmåga att kunna återställa tillgång och tillgänglighet till personuppgifterna. Detta anses enkelt eftersom det sparas säkerhetskopior på de personuppgifter och de behandlingar som utförts så att man ska kunna återställa vid en eventuell incident.

### 5.4.2 Att tänka på vid riskbedömning

Jag ansåg det även befogat att för Erikssons fortsatta riskbedömningar i framtiden utarbeta rutiner för vad de bör tänka på när de identifierar potentiella risker. De som redan tidigare nämnts inkluderas i det dokument med rutiner och riskbedömningsmallen som jag har utarbetat.

De frågor som Erikssons bör tänka på enligt dokumentet är: ”Finns stora problem med faktorer som kan leda till höga sanktionsavgifter?”, ”Finns stora risker för den registrerade med vår behandling?”, Behöver konsekvensutredningar göras beträffande pågående behandling?”, ”Har dataskyddsincidenter inträffat?”, ”Har dataskyddsmyndigheten visat intresse för organisationen?” och ”Saknas struktur som stöder GDPR?”.

# 6 Intervju med personal vid Erikssons

Inför detta kapitel har jag framställt en intervju som utfördes med anställda vid Erikssons. Syftet med denna intervju är främst för mig själv att få mera information om hur GDPR i

praktiken har påverkat företag och de som intervjuas är de som arbetar med personuppgiftshantering hos Erikssons, alltså kommer denna info från personer som direkt blivit insatta i vad dataskyddsförordningen innebär. Intervjun utförs vid samma besök som riskbedömningen utförts och de två kandidaterna som intervjuats intervjuades samtidigt.

Detta är alltså en undersökning med en intervju som tillvägagångssätt. Det finns tre tillvägagångssätt för att bygga upp en intervju. Dessa är:

- Strukturerad intervju vilket betyder att alla frågor är planerade på förhand i vilken alla kandidater ställs samma frågor. Fördelen med denna metod är att den ger en hög säkerhet vid bedömningen.

- Semistrukturerad intervju, en metod inom vilken frågorna är förutbestämda och man själv därefter väljer följdfrågor utifrån vad den intervjuade svarar. Fördel med denna metod är att den intervjuade kan känna sig trygg på så sätt att det inte verkar som ett förhör.

- Ostrukturerad intervju är den metod där kandidaten styr hela samtalet. Fördelen med denna metod är samtalet blir avslappnat som ett intressant samtal mellan intervjuaren och den intervjuade.

(Academicworks, u.d.)

Intervjun är en strukturerad intervju vilket betyder att jag har planerat frågorna på förhand. De frågor som ställs rör sig om hur GDPR har påverkat verksamheten hos företaget och intervjun utfördes på plats vid Erikssons verkstad i Ytteresse och två personer som har auktoritet i företaget ger intervjun.

*Hur har dataskyddsförordningen GDPR påverkat verksamheten?*

Mycket har fortsatt som förr. Programmet DL som fungerar som personuppgiftsbiträde har kartlagt de risker som de identifierat och har kunnat förebygga dessa själva med åtgärder och uppdateringar av programmets skydd.

*Har dataskyddsförordningen medfört kostnader?*

Inga märkbara kostnader har tillkommit med dataskyddsförordningen. De resurser som krävs har vi redan tillgång till och personalen har fått utbildning angående hur man tar sig an dataskyddsförordningen.

*Krävdes stora förberedelser inför dataskyddsförordningen?*

Inte för vår del med tanke på att DL har förberett detta innan förordningen togs i bruk. Den personal som dataskyddsförordningen berör har gått på framförallt DL's utbildning om hur personuppgiftsbehandlingar hädanefter utförs.

*Vilka fördelar och nackdelar har GDPR medfört?*

Inte så mycket, det mesta är nog väldigt likt i jämförelse med hur det var innan. Det ligger ju ett större ansvar på företagets axlar.

*Har det skett förändringar angående hur personuppgifter hanteras?*

Det mesta angående hur vi behandlar personuppgifter har kunnat fortsätta som tidigare. Vi har tagit i bruk en så kallad samtyckesknapp för att den registrerade ska kunna ge sitt samtycke.

*Hur har personalen utbildats angående GDPR?*

Personalen har deltagit i kurser som ordnats för hur man tillämpar GDPR. Detta gäller dock endast den personal som hör till de personuppgiftsansvariga. Övrig personal kommer att få ta del av de rutiner som nyligen utarbetats angående personuppgiftshantering för att även de ska ha kännedom i hur vi hädanefter gör.

*Har det uppstått förändringar i kundrelationerna med dataskyddsförordningen?*

Ingenting märkbart bortsett från hur vi inhämtar samtycke för behandling av deras personuppgifter. Där blev vi tvungna att vidta åtgärder, men i övrigt har inte våra kundrelationer påverkats.

## 6.1 Analys av intervjusvaren

Vad jag fick ut av intervjun är att Erikssons inte har behövt göra så stora anpassningar vad gäller dataskyddsförordningen. Det ERP-program som används, alltså DL, har som personuppgiftsbiträde redan beaktat GDPR i sin mjukvara vilket har underlättat behandlingen för Eriksson. För Erikssons del är alltså DL en pålitlig samarbetspartner när det gäller denna typ av arbete som har beaktat dataskyddsförordningen i och med uppdateringar av mjukvaran.

Personalen har blivit utbildad i hur man tar sig an dataskyddsförordningen av de kurser som DL har ordnat vilket ytterligare underlättade anpassningen. Till programmet som lagrar personuppgifter ges endast tillträde åt de som behöver behandla personuppgifterna för att kunna utföra en tjänst. De rutiner som jag har utarbetat kommer att användas för fortsatt utbildning av personal eftersom det anses viktigt att även de som sällan behandlar personuppgifter inom företaget har en grundläggande kännedom i vad som bör beaktas när de har tillgång till en registrerads personuppgifter.

Naturligtvis har Erikssons nu ett större ansvar på sina axlar än tidigare och därför har koncernen valt att ta till nya metoder för erhållande av samtycke för behandling av personuppgifter. Det har inte kostat mycket då Erikssons redan sen tidigare haft de resurser de behöver för att kunna tillämpa dataskyddsförordningen internt.

Sammanfattningsvis kan alltså konstateras att det för Erikssons del inte krävdes alltför mycket av koncernen med att tillämpa GDPR. I Erikssons fall så har ju personuppgiftsbiträdet gjort en stor del av arbetet. Det i kombination med att man redan innan dataskyddsförordningen togs i bruk har haft ett fungerande system för behandling av personuppgifter vilket gjorde hela genomförandet enklare.

### 6.1.1 Granskning av intervjuns tillförlitlighet

Det första som bör påpekas med intervjun är att den bara utfördes en gång på två av Erikssons personuppgiftsansvariga vilket betyder att den inte bör tolkas som något absolut svar på hur dataskyddsförordningen har påverkat företagens verksamhet i överlag. För en mera tillförlitlig undersökning borde representanter från flera företag av olika storlekar och olika verksamhet ha blivit intervjuade.

Det andra som bör påpekas är att det är en strukturerad intervju som utförts. Det positiva med en sådan intervju är den höga säkerheten vid bedömningen, men ett faktum som kvarstår är att den endast utförs på grund av intervjuarens egna intressen. En strukturerad intervju ger inte utrymme för följdfrågor som en semistrukturerad eller en ostrukturerad intervju ger, utan här besvaras endast de frågor som skrivits ned och det är alltså intervjuaren som håller trådarna.

Jag kunde ha utfört flera intervjuer hos andra företag för en bredare inblick angående GDPR men denna intervju sammanställdes mest på basis av mina egna intressen. Jag valde att utföra endast en intervju, och denna hos Erikssons eftersom jag utförde mitt övriga arbete åt dem.

# 7 Resultat

GDPR röstades igenom redan 2016 och togs i bruk 25:e maj 2018 så företag har haft gott om tid att anpassa sig till förordningen. Erikssons har som tidigare nämnt förberett sig på förordningen genom att delta i utbildningar ordnade av deras personuppgiftsbiträde, DL. Det som jag gjort för dem är att jag utarbetat rutiner åt dem så att de i fortsättningen ska kunna använda det utarbetade dokumentet som riktlinjer för personuppgiftsbehandling. Erikssons arbete med att tillämpa GDPR är inte slut ändå eftersom ständiga uppdateringar behövs för att efterleva denna förordning.

Resultatet av mitt arbete är det att Erikssons nu har rutiner för behandling av personuppgifter som kan användas endera som riktlinjer när man utför personuppgiftsbehandling eller när exempelvis ny personal utbildas angående ämnet.

Vad riskbedömningen beträffar så var det en bra grund för företaget för att de nu ska kunna fortsätta göra sina egna bedömningar och då enklare kunna motarbeta eventuella konsekvenser. Därför var det ett utmärkt tillfälle att utföra en färdigt utarbetad riskbedömning så att personalen har ett exempel på hur en sådan kan gå till utifrån den information som jag delade samt har exempel på möjliga åtgärder för de möjliga riskerna.

Riskbedömningen är en väsentlig del av arbetet som cirkulerar dataskyddsförordningen vilket fick mig att på eget initiativ erbjuda att utarbeta en sådan. Det är viktigt att Erikssons i fortsättningen använder detta material för att själv kunna hänga med i utvecklingen och hålla sig uppdaterade angående risker med personuppgiftsbehandlingar.

Intervjun utfördes för att jag skulle få en bild av vad Erikssons hittills har tagit till för åtgärder för att följa dataskyddsförordningens direktiv. I denna intervju fick jag svar på vad Erikssons hittills har gjort för att tillämpa GDPR. Som nämnts tidigare har DL varit en viktig faktor för deras tillämpning, vilket gör att Erikssons arbete hittills kanske har varit enklare än för övriga organisationer så när som på några mindre åtgärder.

Vad som framkom i intervjun är att det inte krävdes så mycket av Erikssons för att kunna ta i bruk en tillfredsställande tillämpning av GDPR, men ett fåtal förberedelser krävdes naturligtvis.

Angående vad Erikssons har fått ut av mitt arbete så ringdes arbetets beställare upp en sista gång den 3:e maj för en uppdatering. Enligt dem så är syftet med detta arbete att få rutiner,

eller riktlinjer för hur man inom organisationen ska kunna tillämpa GDPR bättre inom Erikssons-koncernen samt att ha material att utgå ifrån när övrig personal utbildas för att få kännedom i vad dataskyddsförordningen kräver. Det anses från deras sida att målet är uppnått och organisationen har tillsvidare en bra sammanfattande genomgång av förordningen och dess tolkningar.

Erikssons behandlar dagligen personuppgifter. Detta arbete har varit en del av det fortsatta arbetet hos Erikssons med deras tillämpning och tolkning av GDPR. Vad som i fortsättningen är viktigt för Erikssons, precis som alla andra organisationer som behandlar personuppgifter är att kunna garantera säkerheten hos de registrerade.

# 8 Diskussion

I detta arbete har jag gett mig in på vad GDPR är och vad det är till för och utgående från det kunnat utarbeta rutiner för ett företag som påverkas av förordningen. I teoridelen gick jag igenom vad dataskyddsförordningen innebär och vilka ändringar som gäller nu som inte tidigare var aktuella. Det har definierats vad personuppgifter är, vilka rättigheter den registrerade har och hur man bör göra vad gäller säkerheten för personuppgifter inom ett företag.

I teoridelen tas det upp om mycket som Erikssons koncernen behöver tänka på i sina rutiner för personuppgiftsbehandling. Teoridelen användes som grund till den empiriska delens innehåll och jag har försökt inkludera allt som är relevant från den samt exkludera sådana delar som inte kom att behöva beaktas vid utarbetningen, detta gäller bland annat behandling av barns personuppgifter, då Erikssons inte behandlar sådana personuppgifter.

I den empiriska delen beskrivs rutiner har utarbetats för behandling av personuppgifter, rutiner för hur Erikssons bör agera när något går fel som när en personuppgiftsincident inträffar, utarbetat och utfört en riskbedömning som innehåller några frågor om vanliga risker angående personuppgifter och utarbetat en till riskbedömningstabell som de kan utgå ifrån när de kartlägger de risker som identifieras med tiden och framställt och utfört en intervju med två personer från företagets ledning för att själv kunna förstå det praktiska med dataskyddsförordningens påverkan. De utarbetade dokumenten, som är resultatet av detta arbete, bör ses som bilagor till detta arbete.

I kapitlet om resultat framkommer vad Erikssons i fortsättningen kommer att tillämpa som rutiner för personuppgiftsbehandlingar. Syftet med mitt arbete är att Erikssons nu har ett underlag för att kunna förenkla sitt arbete. Med hänvisning till teorin kan man se att organisationen följt de hänvisningar som dataskyddsförordningen kräver att man tillämpar, tillika de dokument som utarbetats åt den.

GDPR ger inga konkreta exempel på vad en organisation bör göra för att uppfylla de krav som ställs så mycket vad gäller åtgärder lämnas till egen tolkning. En ny tillämpning för Erikssons är att se hur läget är med den interna kontrollen, det vill säga se vilka rutiner som härefter bör tillämpas. Säkerheten är viktig att kolla upp till vilket jag hoppas att de verktyg de nu har kommer att användas. Till sist kan sägas ännu en gång att det för Erikssons del inte krävts så stora förändringar i och med att man redan tidigare haft ett system vad gäller personuppgiftsbehandlingar.

Mitt arbete har gett mig en bra översikt angående vad som gäller med dataskyddsförordningen. Att påbörja arbetet var lite knepigt eftersom jag inte tidigare på något sätt hade bekantat mig med GDPR så jag fick starta från grunden. Personalen på Erikssons har varit hjälpsam angående det av DL framställda material som jag fick låna för att få en inblick av hur GDPR kan tillämpas. Det i kombination med de böcker som jag lånat och de webbsidor jag besökte gjorde att mitt arbete ändå kunde framskrida i god ordning.

En sak jag borde ha gjort annorlunda var att utarbeta och utföra intervjun först av allt arbete, eftersom jag då skulle ha haft det enklare att utarbeta rutinerna än vad jag hade nu. Situationen var dock den att Erikssons ville ha rutiner och jag ville se över vad detta innebar så jag började med att läsa på. Intervjun skulle ha gett en bättre grund för hur jag skulle börja, men i slutändan är jag ändå nöjd med resultatet. Orsaken till att jag valde att göra en intervju var av mitt eget intresse, alltså för att bättre kunna förstå tillämpningen av GDPR inom ett företag. Det förklarar också varför jag valde att göra det i formen av en strukturerad intervju, vilket oftast är just för intervjuarens egna intresse.

Riskkartläggningen tog jag eget initiativ till efter att ha läst mig in på ämnet, eftersom jag ville ha ett mera varierande innehåll i arbetet och eftersom säkerheten är en väsentlig del vid tillämpningen av GDPR och det just därför är viktigt att identifiera möjliga risker. Det material jag hade beskriver riskbedömningen tillräckligt bra för att jag skulle känna mig säker på att kunna utföra den.

Vad jag har lärt mig av detta arbete är det väsentliga vad gäller dataskyddsförordningen GDPR och att kunna tillämpa detta i en organisation. Jag har fått ta del av många aspekter och definitioner som GDPR kretsar kring (som definitionen på personuppgifter, samtycke, register, personuppgiftsansvarige med mera) och hoppas att Erikssons ska kunna ha bra nytta av detta samt hoppas jag att läsare av detta arbete också ska kunna dra nytta av all denna information.

# 9 Källförteckning

Academicwork, u.d.. Academicwork – 3 intervjutekniker-vilken väljer du? [Online]
Available at: https://www.academicwork.se/insights/arbetsgivare/intervjutekniker
[Accessed 04 2019]

Datainspektionen, u.d.. Datainspektionen - Föra register över behandling. [Online]
Available at: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/foraregister-over-behandling/ [Accessed 03 2019]

Datainspektionen, u.d.. Datainspektionen – Samtycke [Online]
Available at: https://www.datainspektionen.se/lagar-regler/dataskyddsforordningen/rattslig-grund/samtycke/
[Accessed 03 2019]

Datainspektionen, u.d. Datainspektionen – Hantera personuppgifter i E-post [Online]
Available at: https://www.datainspektionen.se/lagar-regler/dataskyddsforordningen/samma-regler-for-alla/hantera-personuppgifter-i-e-post/
[Accessed 03 2019]

DL Software, u.d. DL Software – Hemsida [Online]
Available at: http://www.dlsoftware.se/sv/hemsida/
[Accessed 03 2019]

Erikssons, u.d.. Erikssons-framsida. [online]
Available at: https://www.erikssons.fi/sv/framsida/
[Accessed 03 2019]

GDPR, 2016. GDPR [Online]
Available at: https://www.gdpr.associates/wp-content/uploads/2017/05/Swedish-CONSIL3AST_5419_2016_INIT3ASV3ATXT.pdf
[Accessed 03 2019]

Frydlinger, D & Edvardsson, T & Olstedt Carlström, C & Beyer, s., 2018. GDPR: Juridik, Organisation och säkerhet enligt dataskyddsförordningen. Stockholm: Norstedts juridik Ab.

Wendleby, M. & Wetterberg, D., 2018. Dataskyddsförordningen GDPR: Förstå och tillämpa i praktiken. Stockholm: Sanoma Utbildning Ab.

# 10 Bilagor

**Bilaga 1 – Rutiner för behandling av personuppgifter**

# RUTINER FÖR BEHANDLING AV PERSONUPPGIFTER

Erikssons

Johan Sundqvist
Johan.sundqvist@edu.novia.fi

# Rutiner för behandling av personuppgifter

Viktigt att alltid tänka på är att allt som rör personuppgifter räknas som behandling av dessa, detta inkluderar passiv lagring.

1. Varje behandling av personuppgifter bör ske i enlighet med den rådande lagstiftningen.
2. Personuppgiftsansvarige är skyldig att se till att dataskyddsförordningen följs.
3. Erhållande av samtycke bör kunna bevisas. Därför är det viktigt att vi får en underskrift vid insamling av personuppgifter. Samtycke bör ges entydigt och klart. Passivitet får inte godkännas som samtycke och ett samtycke bör kunna dras tillbaka när som helst. Kom ihåg att dokumentera samtycket.
4. Vad är syftet med behandlingen av personuppgifter? Detta bör klargöras för kunden på ett lättförstått sätt. Kunden bör ha möjlighet att godkänna varje del för sig samt välja bort de delar som denne inte är intresserad av. Syftet kan vara en eller flera av följande:
    - Att administrera kundförhållandet
    - Marknadsföring
    - Säkerhetsfrågor
    - Att tillåta reklam från andra samarbetspartners eller andra koncernbolag
    - Att lämna ut uppgifter till samarbetspartner
    - Affärs- och metodutveckling
5. Personuppgifter får inte behandlas i annat syfte än det vi har kommit överens om med den registrerade.
6. För register över personuppgiftsbehandlingen. Detta innebär att vi dokumenterar personuppgiftsbehandlingen som utförts i DL. För en dokumentering på registret, över dess uppgifter och dess användningsändamål
7. Åtkomst till personuppgifterna bör begränsas till endast de som är behöriga.
8. Håll personuppgifterna korrekta och uppdaterade. Om det framkommer att personuppgifterna har ändrats så ändrar vi på dem.
9. När den registrerades personuppgifter inte längre kommer att behövas, eller på den registrerades begäran ska de raderas och förstöras.
10. Samla inte in flera personuppgifter än de som behövs. Personuppgifter som inte behövs tas beslut om angående radering.

11. Förhindra personuppgifts- och dataskyddsincidenter. Om sådana inträffar bör vi vidta de åtgärder som tydliggörs i kapitlet ”Om något går fel”.
12. Tydliggör rättigheterna får den registrerade. Den registrerades rättigheter framkommer nedan.

## Den registrerades rättigheter

Vid Erikssons behöver vi kunna beakta den registrerades rättigheter. Dessa är:

### Rätten till information

Den registrerade har rätt till att få information. Denna information bör vara tillgänglig, ingående och klar. Blir vi tillfrågade angående information bör vi kunna ge ut skriftligen enligt följande punkter:

- Personuppgiftsansvarig, kontaktperson och kontaktuppgifter
- Behandlingens ändamål och juridiska grund
- Mottagare av personnummer
- Flytt till länder utanför EU
- Lagringstid eller kriterier för borttagande
- Information om den registrerades rättigheter
- Information om automatiserat beslutstagande och profilering.

Det exakta innehållet beror på varifrån informationen har samlats.

### Rätten att få tillgång till uppgifterna

- Personuppgiftsansvarige har skyldighet att ge en kopia av de uppgifter som behandlas.
- Uppgifterna bör ges skriftligen eller via den elektroniska kanal (DL) som används för kontakt.
- Uppgifterna bör ges inom trettio (30) dagar.

DL Prime har en funktion för att skapa textfiler över kunduppgifterna som finns där. Använd den.

### Rätten till korrigering av uppgifter

- Den personuppgiftsansvarige har skyldighet att korrigera felaktiga uppgifter och meddela detta till mottagare.
- Det finns en skyldighet för att se till att personuppgifter är korrekta. Om detta upptäcks så ändrar vi uppgifterna och om detta inte går så tar vi bort dem, genom radering och förstörelse av personuppgifterna.

## Rätten att bli glömd

Den registrerade har rätt att bli glömd, vilket innebär att dennes personuppgifter tas bort om

- De inte längre behövs för det ursprungliga ändamålet
- Den registrerade drar tillbaka sitt samtycke, och ingen annan grund finns för att ha dem kvar
- Den registrerade motsätter sig behandlingen på godtagliga grunder.

I DL Prime kan man ta bort händelser och personer som det inte längre finns behov för. Man kan även anonymisera alla händelser för en enskild kund.

## Rätten till begränsad behandling

Den registrerade har rätt att kräva att personuppgiftsansvarige begränsar behandlingen om

- Den registrerade anser att uppgifterna är felaktiga, varefter riktigheten kontrolleras
- Behandlingen är lagstridig, men den registrerade ger rätt till begränsad behandling istället för borttagning
- Den personuppgiftsansvarige inte längre behöver uppgifterna för ändamålet i fråga, men den registrerade behöver dem för att säkra sina juridiska rättigheter.

I DL kan man sätta in en varning till kundkortet. På detta sätt kan vi säkerställa att personuppgifterna inte får behandlas för andra ändamål.

## Rätten till dataportabilitet

Den registrerade har rätt till dataportabilitet, d.v.s. rätt att få sina personuppgifter i ett organiserat, allmänt använt och maskinläsbart format och få personuppgifterna flyttade elektroniskt till en annan personuppgiftsansvarig om så är möjligt.

Detta om behandlingen baserar sig på samtycke eller avtal och behandlingen görs med automatik, alltså elektroniskt. Dessa krav uppfylls med DL Prime eftersom ett textdokument som skapas i detta program är organiserat, maskinläsbart och i standarformat.

## Rätten att få information om dataskyddsincidenter

- Den personuppgiftsansvarige har skyldighet att meddela myndigheter och registrerade om dataläckor.
- Detta gäller även om personuppgifter förstörs i misstag eller lagstridigt, ändras av utomstående eller om utomstående får tillgång till eller stjäl personuppgifter

- Tidsfristen för att meddela om detta är 72 timmar från det att vi blivit medvetna om eventuell incident.

Om en dataskyddsincident inte är en risk för den registrerade så har vi ingen anmälningsskyldighet till den registrerade. Alla incidenter bör dock dokumenteras och i dokumentationen bör det ingå orsaker, påverkande faktorer, resultat och åtgärder.

Om en misstänkt dataskyddsincident inträffar i DL-programmet så bör detta även meddelas åt DL så snabbt som möjligt.

## Ifall något går fel

### Personuppgiftsincident

Ifall en personuppgiftsincident inträffar så vidtar vi följande åtgärder:

- 72 timmar från att vi upptäckt en personuppgiftsincident så meddelar vi om detta till dataskyddsmyndigheten.
- Om incidenten innebär stora risker så informerar vi också den eller de registrerade som utsatts för incidenten. Beskriv tydligt och klart incidentens art och ha med kontaktuppgifter till den kontaktpunkt varifrån mera information kan erhållas. Beskriv i denna information de sannolika konsekvenserna och de åtgärder vi vidtagit för att åtgärda incidenten. Lämna också rekommendationer till den registrerade om eventuella säkerhetsåtgärder om hur de negativa effekterna kan mildras.
- Meddela också personuppgiftsbiträdet DL om dataskyddsincidenter.
- Vi dokumenterar alla personuppgiftsincidenter. Denna dokumentation bör innefatta incidentens omständigheter, dess effekter och de korrigerade åtgärder som vi vidtagit. Detta för att dataskyddsmyndigheten enklare ska kunna se att vi efterlever dataskyddsförordningen.
- Anteckna även alla kontakter och råd vi får från dataskyddsmyndigheten.
- Om anmälan görs senare än 72 timmar från att vi upptäckt incidenten så bör vi lämna in en orsak angående varför vi är försenade.
- Om vårt personuppgiftsbiträde (DL) råkar ut för en incident är den skyldig att anmäla åt oss för att vi ska kunna fullgöra våra plikter.

## Riskbedömning – Att tänka på

Nedan har framställts riktlinjer för riskbedömning. Dessa riktlinjer är vad vi bör tänka på vid Erikssons när vi utför riskbedömningar i fortsättningen, eftersom en riskbedömning inte bara utförs en gång utan är en pågående handling. För riskbedömningstabellen, se bilaga.

- Finns stora problem med faktorer som kan leda till höga sanktionsavgifter?
- Finns stora risker för den registrerade med vår behandling?
- Behöver konsekvensutredningar utföras gällande pågående behandling?
- Har dataskyddsincidenter inträffat?
- Har dataskyddsmyndigheten visat intresse för organisationen?
- Saknas struktur som stöder GDPR?

**Bilaga 2 – Riskbedömningstabell - Print**

| Identifierad risk + möjlig åtgärd | Sannolikhet | Konsekvens | Riskfaktor |
|---|---|---|---|
| | 1-5 | 1-5 | 1-25 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Bilaga 3 – Riskbedömningstabell – Excel**

| Identifierad risk + möjlig åtgärd | Sannolikhet | Konsekvens | Riskfaktor |
|---|---|---|---|
| | 1-5 | 1-5 | 1-25 |
| | | | 0 |
| | | | 0 |
| | | | 0 |
| | | | 0 |
| | | | 0 |
| | | | 0 |
| | | | 0 |
| | | | 0 |