EXAMENSARBETE

Den nya Dataskyddsförordningen

Om småföretagares compliance med GDPR

Annelie Olofsson

Rättsvetenskap, kandidat
2018

Luleå tekniska universitet
Institutionen för ekonomi, teknik och samhälle

LULEÅ TEKNISKA UNIVERSITET

Sammanfattning

På grund av brister i lagstiftningen beslöt Europaparlamentet och EU:s ministerråd år 2016 att en ny förordning rörande hantering av personuppgifter skulle råda i Europeiska unionen från och med den 25 maj 2018. Denna förordning kallas GDPR och kommer ersätta PUL. Förordningen innehåller bland annat krav på principer som måste följas vid behandling av personuppgifter, de rättsliga grunder som användas för laglig personuppgiftsbehandling så som samtycke från den registrerade samt redogörelse för de olika ansvarsrollernars skyldigheter. GDPR kommer innebära att Datainspektionen får ett utökat uppdrag som bland annat kan resultera i utdömandet av höga sanktioner om behandlingen inte utförs i enlighet med förordningen. Uppsatsen fastställer gällande rätt vid behandling av personuppgifter efter GDPR, samt undersöker hur företag kan förbereda sig inför förändringen och hur många småföretag som faktiskt är förberedda en månad innan införandet. För att besvara syftet har i första hand en rättsdogmatisk metod använts. Denna har kompletterats med en kvalitativ undersökning. Den nya förordningen kommer att påverka alla företag, därav måste alla småföretag sätta in sig i de nya reglerna och undersöka hur de hanterar personuppgifter och hur de ska gå till väga för att hanteringen ska vara laglig. Två olika undersökningar presenteras, dels en undersökning utförd av Visma två månader innan GDPR träder i kraft, dels undersökning inom ramen för denna uppsats utförd en månad innan införandet av förordningen. Båda studierna pekar på att många småföretagare är dåligt förberedda och resultatet från den undersökning som utförts inom ramen för uppsatsen visar att många företag inte har satt sig in i de nya reglerna.

Innehållsförteckning

1. Inledning

Utvecklingen inom IT går i extremt snabb takt. Konsekvensen av detta blir att lagar och förordningar inte hinner med. Man skulle kunna säga att rättsregleringen inte har varit uppdaterad och därför inte heller speglat verkligheten vi lever i. Den nuvarande regleringen är främst anpassad för papper och kan således inte direkt appliceras på den digitala sfären. Läget har varit oklart och många vet inte vad som gäller för den digitala informationen. Det blir också problematiskt då det inte har funnits en allmän giltighet för regleringen och olika länder har haft olika regleringar. Människor delar ut information och vet egentligen inte var den i slutändan tar vägen. Vi är därför i stort behov av ett skyddsnät som ger oss tillbaka kontrollen över våra personuppgifter.[1]

Den snart obsoleta personuppgiftslagen (1998:204) (PUL) bygger på EU-direktivet Data Protection Directive (DPD) från år 1995. PUL var uppbyggd utifrån DPDs innehåll och sammansättningens struktur.

År 2012 introducerade Europeiska kommissionen ett förslag till nya regler för dataskydd och personuppgiftsbehandling. Syftet var att modernisera reglerna i DPD och att tillämpningen skulle vara mer enhetlig inom EU. Europaparlamentet och EU:s ministerråd antog år 2016 dataskyddsförordningen General Data Protection Regulation (GDPR), och denna kommer bli gällande rätt den 25 maj 2018 och kommer således att ersätta PUL och gäller i samtliga medlemsländer.[2] GDPR är striktare än PUL och de som behandlar personuppgifter får nu ett större ansvar. Bland annat ställer GDPR ett högre krav på informationsgivning, samtycke samt anmälan vid incidenter.

I regeringens proposition till GDPR har både *Företagarna* och *Småföretagarnas Riksförbund* utryckt en oro för gruppen småföretagare, dels för de ökade kostnaderna samt administrativa bördor för de nya rutiner som måste införas.[3] I Sverige fanns under 2017 34 117 småföretag,[4] det vill säga företag med mellan 10-49 anställda.[5] Dessa företag utgör en stor del av samhället och främjar sysselsättning, ekonomisk tillväxt och innebär social stabilitet för många människor.[6] Samtidigt är småföretagen också den grupp som, på grund av bristande medel och kunskap, kanske blir mest påverkade av en ny reglering. De måste göra anpassningar i sina system och rutiner för att klara av de nya kraven och undvika de stränga sanktionerna.[7] Det finns dock indikationer som tyder på att småföretagen inte är förberedda trots att GDPR snart träder ikraft. Frågan är hur småföretag bör förbereda sig inför förändringarna och hur många som är i fas när det gäller att sätta sig in och anpassa sig efter GDPR:s regleringar.

1.1 Syfte

Uppsatsens syfte är att med fokus på småföretagare först genomföra en översiktlig kartläggning av rättsläget efter att den nya dataskyddförordningen trätt i kraft. Vidare är syftet att undersöka hur småföretagare kan förbereda sig inför ikraftträdandet av GDPR. Slutligen är uppsatsens syfte att undersöka om småföretagare är i fas vad det gäller anpassningsarbetet inför GDPR.

[1] GDPR. Skäl 6.
[2] GDPR. Artikel 99.
[3] Prop. 2017/18:105, s 180 f.
[4] Ekonomifakta. *Företagens storlek*.
[5] Kommissionens rekommendation 2003/361/EG, Artikel 2.2.
[6] Användarhandledning om definitionen av SMF-företag s 3.
[7] Lindström, A. Svenska Dagbladet. *Småföretagare hotas av miljonböter: ”Skrämmande”*.

Följande konkreta frågeställningar behandlas i uppsatsen:

- I stora drag, hur ser gällande rätt ut för vid behandling av personuppgifter efter GDPR.
- På vilket sätt kan småföretagen arbeta mot förändringarna, vad behöver göras?
- Är småföretagen i fas när det gäller anpassning inför den nya regleringen?

1.2 Metod

För att undersöka de två första frågeställningarna som berör rättsläget efter införandet av GDPR samt vad som behöver göras inför införandet av GDPR, har jag lutat mig mot den rättsdogmatiska metoden. En utgångspunkt för att använda denna metod är att främst koncentrera sig på de allmänt accepterade rättskällorna så som förarbete, lagtext, praxis och doktrin.[8] Denna uppsats tar till stor del sin utgångspunkt i den kommande lagtexten då praxis och doktrin har varit begränsat vid tidpunkten för författandet då GDPR ännu inte trätt i kraft. Utöver detta har bland annat publikationer och utlåtande från svenska myndigheter används, så som Datainspektionen samt verksamt.se som är ett samarbete mellan flera myndigheter (bland annat skatteverket, bolagsverket och tillväxtverket). Den information som återfinns hos dessa aktörer är främst riktat till allmänheten och inte till yrkesverksamma jurister. Datainspektionen är dock den ansvariga tillsynsmyndighet i Sverige och har därför funnits intressant då det materialet kan användas för vägledning.

1.2.1 Vismas undersökning

I del 5 användes en kvalitativ undersökning för att undersöka om småföretag har förberett sig och anpassat sig i enlighet med förordningen. Visma spcs (Visma) har genomfört en undersökning där de skickade ut frågor via mail till deras kunder inom gruppen småföretagare. Frågorna som ställdes var;

- *Den 25 maj träder EU:s nya dataskyddsförordning GDPR i kraft. Har du satt dig in i vad de nya reglerna för skydd av personuppgifter innebär för ditt företag?*
- *Har du vidtagit några konkreta åtgärder i ditt företag med anledning av GDPR, till exempel GDPR-säkrat kundregistret eller raderat gamla personuppgifter om eventuella medarbetare?*

Undersökningen skickades ut till 18 000 småföretagare men endast 965 företag valde att besvara undersökningen. Detta ger en svarsfrekvens på ca. 5%.

1.2.2 Min undersökning

Då Vismas undersökning inte kan ses som en korrekt spegling av verkligheten på grund av den låga svarsfrekvensen bestämde jag mig för att utföra en undersökning i Norrbottens län. Via hemsidan ”allabolag.se” sållade jag fram 519 företag efter att ha begränsat mig till småföretagare (jag valde 10–19 anställda) och endast aktiebolag. Jag beslöt mig för att kontakta 30 stycken företag och valde därför ut vart sjuttonde företag på denna lista. Jag tog därefter kontakt via telefon och mail med människor i VD-position eller chefsposition. Jag började kontakta via telefon och de jag ej fick tag på skickade jag ett mail till med frågorna. Om jag inte fått svar efter denna process skickades ett påminnelsemail efter ca. 5 dagar med frågorna igen. Frågorna jag ställde var;

- *Har ni på (förtagets namn) satt er in i vad de nya reglerna innebär för ert företag?*
- *Om ja, har ni gjort några konkreta åtgärder med anledning av reglerna?*

[8] Korling, F & Zamboni M. Juridisk metodlära, s 21.

Mitt bortfallsantal blev 4 stycken, alltså blev svarsfrekvensen 86%. 2 stycken företag fick jag ej tag på, ett annat företag svarade att de inte ville medverka och det fjärde företaget svarade på mitt mail med ett blankt mail.

1.3 Disposition

Uppsatsen tar avstamp i en redogörelse för den gällande rätten efter införandet av den nya dataskyddsförordningen (2). Efter det beskrivs de viktigaste skillnaderna mellan GDPR och PUL mer ingående med fokus på lagtexten (3). Vidare över till en presentation av situationer där det exemplifieras när företag hanterar personuppgifter samt sedan en redogörelse för hur företag ska gå till väga för att anpassa sig till de nya reglerna (4). Efter det redovisas Vismas undersökning som följs av resultatet från min undersökning (5). Till sist analyseras och diskuteras det som framkommit i de tidigare kapitlen (6).

2. Den nya dataskyddsförordningen GDPR

I detta kapitel redovisas dataskyddsförordningens viktigaste bestämmelser för företag vad gäller personuppgiftsbehandling. Detta innebär att bestämmelser som gällde i PUL också kommer beskrivas och viktiga nyheter kommer poängteras.

2.1 Bakgrund

Att reglerna givits i en förordning innebär att de blir direkt gällande i alla medlemsländer efter att den antagits av EU utan att inkorporeras eller transformeras till nationella rättsregler. En förordning gäller lika för alla och får således inte lagstiftas sämre än vad som följer av förordningen, det får däremot lagstiftas till det bättre, i det här fallet strängare för de som behandlar personuppgifter.[9]

Målet med GDPR är att säkerställa en skyddsnivå som är enhetlig för alla fysiska personer samt att den ska undanröja skillnader inom EU som kan påverka det fria flödet av personuppgifter negativt på den inre marknaden.[10] Den enskildas rätt till kontroll över sina personliga uppgifter finns även stadgat som en av de grundläggande rättigheterna genom skyddet av den personliga integriteten i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna[11] samt i artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF).[12] Rätten till skydd för den personliga integriteten finns även grundlagsstadgat i Sverige.[13]

GDPR är ett medel som är till för att skydda personlig information, och den stärker de enskildas rättigheter gentemot de som behandlar personuppgifter och de som ansvarar för behandlingen (personuppgiftsansvariga).[14]

2.2 Personuppgift

Den juridiska definitionen på personuppgift i GDPR är:

”varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”.[15]

Detta innebär att all slags information som kan anknytas till en levande specifik person är en personuppgift och det som krävs är att en fysisk person kan identifieras med hjälp av uppgifterna. Det kan förslagsvis vara namn, personnummer, adress, ljudupptagningar, bilder eller kundnummer. Vissa uppgifter blir personuppgifter när de sammankopplas med varandra. Exempelvis så säger efternamnet Andersson inget om en specifik person, men när detta sammankopplas med exempelvis en adress så blir det en personuppgift. Även uppgifter som har kodats,

[9] Bernitz, U & Kjellgren, A. Europarättens grunder, s 55.
[10] GDPR. Skäl 13.
[11] Europeiska unionens stadga om de grundläggande rättigheterna 2010/C 83/02.
[12] EUF 2012/C 326/01.
[13] Regeringsformen 2 kap. 6§.
[14] GDPR. Skäl 11.
[15] GDPR. Artikel 4.1.

pseudonymiserats eller krypterats men som med hjälp av kompletterande uppgifter kan hänföras till en person är personuppgifter.[16]

Vissa uppgifter har beklätts med ett extra starkt skydd genom förordningen då de anses som särskilt känsliga. Exempel på särskilt känsliga uppgifter är sådana uppgifter som kan avslöja ras, etniskt ursprung, politisk åsikt, religiös övertygelse, genetiska och biometriska uppgifter eller sexuell läggning. Huvudregeln för sådana uppgifter är att de är förbjudna att behandlas om det inte finns ett samtycke. Det finns alltså inte utrymme för annan rättslig grund (se nedan avsnitt 2.5) när det gäller behandling av särskilt känsliga uppgifter som det finns för andra typer av personuppgifter.[17]

2.3 Behandling

Behandling definieras i förordningen som:

”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring”.[18]

Den behandling som berörs är den som sker helt eller delvis via automatisk behandling samt manuell behandling av personuppgifter som ingår eller är avsedda att ingå i ett register. Med automatisk behandling menas sådan behandling som sker via datorer eller annan digital teknik. För att GDPR ska vara tillämplig på manuell behandling krävs som nämnt ovan att uppgifterna ingår eller ska ingå i ett register.[19] Ett register kan definieras som en strukturerad samling av personuppgifter, uppgifterna ska vara sorterade i ett system som möjliggör att man kan söka bland uppgifterna. Exempelvis uppfyller inte en pappershög på ett skrivbord kriterierna för att vara en strukturerad samling och därmed är GDPR inte applicerbar.[20]

2.4 Principer för behandling av personuppgifter

Artikel 5 i förordningen slår fast vissa grundläggande principer som gäller för all behandling av personuppgifter, dessa ska vara uppfyllda när personuppgifter behandlas. Dessa principer motsvarar de krav som fanns i PUL, men innehåller även en viktig nyhet som uttryckligen anger att den personuppgiftsansvarige har ansvar för att kunna visa att dessa principer följs.[21]

- *Laglighet, Korrekthet och Öppenhet*

I förhållande till den person som behandlas (fortsättningsvis kallad den registrerade) ska uppgifterna behandlas lagligt och korrekt utifrån den gällande rätten. Bestämmelsen uttrycker att personuppgifter bara får behandlas så som är angivet i förordningen eller annan lagstiftning. Öppenhetsprincipen ger de enskilda rätt till att informationen och kommunikationen är lättillgängliga och lättbegriplig samt att språkbruket ska vara enkelt och tydligt. Det är av stor vikt att det tydligt framgår i informationen vem den personuppgiftsansvarige är, hur personuppgifter

[16] Datainspektionen. *Personuppgifter och personuppgiftsbehandling*.
[17] GDPR. Artikel 9.1, artikel 9.2a.
[18] GDPR. Artikel 4.2.
[19] GDPR. Artikel 2.1.
[20] Datainspektionen. *Personuppgifter i arbetslivet*.
[21] Datainspektionen. *Principer för behandling av personuppgifter*.

har samlats in, hur de används och vad syftet med behandlingen är. Den registrerade ska även informeras om risker, regler och rättigheter i samband med personuppgiftshanteringen.[22]

- *Ändamålsbegränsning*

Insamling av personuppgifter får endast ske för ändamål som är berättigade och som har varit uttryckligt angivna. Ändamålet med behandlingen ska vara tydligt innan insamlingen av uppgifterna påbörjades. Den registrerade måste således ha fått information i förväg om ändamål och ändamålet får inte ändras i efterhand utan att den registrerade har fått information om detta. Det finns några specifika fall där det är godtaget att använda de insamlade uppgifterna till ett annat ändamål, exempel kan vara om den nya behandlingen är förenlig med det ursprungliga ändamålet som de samlades in för, eller om det handlar om att fullfölja en uppgift av allmänt intresse eller vid myndighetsutövning som den personuppgiftsansvarige har fått som uppdrag.[23]

- *Uppgiftsminimering*

Insamlade uppgifter måste vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål som de samlades in för. Detta innebär att det inte är acceptabelt att behandla uppgifter utan en legitim anledning.[24] De får alltså inte samlas in för framtida möjliga behov.[25]

- *Korrekthet*

Uppgifterna som finns registrerade ska vara korrekta och måste därför vara uppdaterade. Den personuppgiftsansvarige har därför ett ansvar att vidta rimliga åtgärder för att säkerställa att personuppgifter som är felaktiga rättas eller raderas utan dröjsmål.[26]

- *Lagringsminimering*

Lagring av personuppgifter får inte ske en längre tid än vad som är nödvändigt för ändamålet i en form som gör det möjligt att identifiera de registrerade. När uppgifterna inte längre behövs ska de raderas eller avidentifieras om det ska sparas exempelvis för arkivändamål eller allmänt intresse.[27]

- *Integritet och Konfidentialitet*

Det är av stor vikt att personuppgifter skyddas och därför måste det finnas lämpligt skydd så att inte obehöriga kan komma i kontakt med uppgifterna och för att det inte ska ske obehörig användning av uppgifterna. De ska även skyddas mot otillåten behandling, förlust och det ska finnas lämpligt skydd så att de ej kan skadas via förstöring eller skadas genom olyckshändelse.[28]

- *Ansvarsskyldighet*

Ansvarsskyldigheten är en viktig nyhet i förordningen. Den innebär att personuppgiftsansvariga har ansvar över att se till att de uppsatta principerna följs. De ska dessutom kunna visa för Datainspektionen hur principerna efterlevs. Den personuppgiftsansvarige ska kunna bevisa att lämpliga tekniska och organisatoriska åtgärder har genomförts och att dessa uppdateras vid behov. Dessa interna rutiner ska finnas beskrivet i en dataskyddspolicy.[29] Ett sätt som företag

[22] GDPR. Artikel 5.1a, Skäl 39.
[23] GDPR. Artikel 5.1b, artikel 14.4, skäl 50.
[24] GDPR. Artikel 5.1c, skäl 39.
[25] Datainspektionen. *Uppgiftsminimering*.
[26] GDPR. Artikel 5.1d.
[27] GDPR. Artikel 5.1e.
[28] GDPR. Artikel 5.1f.
[29] GDPR. Artikel 5.2, skäl 82. Datainspektionen. *Ansvarsskyldighet*.

kan visa att de följer förordningen är genom att använda sig utav godkända uppförandekoder (godkända branschstandarder) eller godkända certifieringsmekanismer. Syftet med den här principen är att öka efterlevnaden av reglerna.[30]

2.5 Rättslig grund för behandling av personuppgifter

I Artikel 6 anges en uttömmande lista över de olika rättsliga grunder som får föreligga för att behandling av personuppgifter ska vara laglig. Denna lista skiljer sig inte nämnvärt ifrån den som fanns i PUL, dock får den rättsliga grunden samtycke en snävare betydelse och innehåller fler krav.

2.5.1 Samtycke

Ett samtycke är individuellt och kan endast lämnas av den berörda personen. Ett samtycke bär också rättigheten att när som helst kunna dras tillbaka vilket innebär att en framtida behandling av uppgifterna inte längre får ske. En stor nyhet i GDPR är att ett samtycke ska läggas fram på ett klart och tydligt språk.[31] Ett lämnat samtycke ska alltid ske frivilligt och vara en otvetydig viljeyttring. Det är inte accepterat att ett samtycke ges via passivitet. Samtycket ska vara specifik till behandlingen och den ska vara informerande. Detta innebär att den som ska samtycka måste få veta i förväg vad det är den samtycker till, åtminstone måste personen i förväg ha kunnat ta reda på vad den samtyckt till och få veta syftet med insamlingen samt om det kommer spridas vidare. Informationskravet har stärkts i förordningen genom att den som samlar in personuppgifter måste kunna klargöra för hur, när och för vilka syften som de insamlade uppgifterna används.[32] Om behandlingen kommer tjäna flera olika ändamål ska separata samtycken ges för varje ändamål.[33] Ett samtycke som ingår i ett mer omfattande avtal ska tydligt särskilj från de andra frågorna.[34]

2.5.2 Samtyckens former

Förordningen innehåller inte några specifika regler för formkrav på samtycken. Det enda som krävs är att det ska kunna bevisas att ett samtycke föreligger. Detta innebär i praktiken ett dokumentationskrav för de som behandlar personuppgifter.[35]

2.5.3 Andra rättsliga grunder för behandling

I förordningen räknas fem villkor upp där samtycken inte behövs för behandling av personuppgifter. De har rättslig grund utan ett samtycke. Villkoren är uttömmande så en behandling är inte laglig om ingen av dessa villkor föreligger.[36]

- Det första villkoret är när behandlingen krävs för att kunna fullgöra ett avtal där den ena parten är den registrerade eller för åtgärder som måste ske innan ett avtal kan ingås.[37] Exempel på sådan behandling kan vara när företaget samlar personuppgifter för att kunna fakturera kunden.[38]

[30] GDPR. Artikel 24, skäl 74.
[31] GDPR. Artikel 7.
[32] GDPR. Artikel 4.11, skäl 32.
[33] GDPR. Skäl 32.
[34] GDPR. Artikel 7.2.
[35] GDPR. Artikel 4.11, skäl 42.
[36] Prop. 2017/18:105, s 104.
[37] GDPR. Artikel 6.1b.
[38] Datainspektionen. *Avtal med den registrerade*.

- Det andra villkoret berör när behandlingen är nödvändig för den personuppgiftsansvarige för att denne ska kunna fullgöra en rättslig förpliktelse.[39] En rättslig förpliktelse är sådant som följer av lag exempelvis av bokföringslagen.[40]

- Det tredje är för tillfällen när behandlingen behövs för att skydda intressen som är av betydelse för den registrerade,[41] så som akut sjukvård.[42]

- Det fjärde handlar om behandling som är behövlig för det allmänna intresset eller i myndighetsutövning.[43] Detta aktualiseras främst för situationer som rör myndigheter.[44]

- Det femte och sista villkoret berör behandlingar som är nödvändiga för ett ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intresse och dessa väger tyngre än den registrerades intressen av att inte behandlas, en så kallad intresseavvägning. Denna är dock ej applicerbar på de uppgifter som är att anse som särskilt känsliga.[45] Detta kan exempelvis föreligga om den registrerade är anställd av den personuppgiftsansvarige.[46]

2.6 De enskildas stärkta rättigheter i GDPR

I förordningen följer ett antal rättigheter som bärs av den registrerade, dessa rättigheter har nu utökats och specificerats jämfört med PUL. Dessa följer nedan och beskrivs utifrån de olika avsnitten i förordningen som rör den registrerades rättigheter.

- *Insyn och villkor*

Det råder en öppenhetsprincip som innebär att den personuppgiftsansvarige alltid ska informera och kommunicera med den registrerade på ett lättåtkomligt, kortfattat och begripligt sätt. Den registrerade har rätt att få information om när behandling av personuppgifter sker. Detta ska tillhandahållas skriftligt, men kan också ske muntligt om den registrerade begär det. Den personuppgiftsansvarige ska även underlätta för den registrerade att utöva sina rättigheter.[47]

- *Information och tillgång till personuppgifter*

I förordningen görs en uppdelning mellan personuppgifter som samlats in från den registrerade och som samlats in från annan part. Oavsett var uppgifterna kommer ifrån ska den registrerade informeras om de uppgifter som blivit behandlade. Den personuppgiftsansvarige har många liknande skyldigheter i båda fallen, men i de fall som uppgifterna kommer från en annan part ska den personuppgiftsansvarige förse den registrerade med uppgifter som berör parten som uppgifterna kommit ifrån. Den registrerade har i båda fallen alltid rätt att få identiteten och kontaktuppgifter till den personuppgiftsansvarige. Den personuppgiftsansvarige ska även utge information om syftet, den rättsliga grunden och om uppgifterna kommer att lämnas till andra mottagare och vilka de mottagarna är. De ska även försäkra att behandlingen sker rättvist samt hur länge uppgifterna kommer lagras. Den registrerade ska få en kopia på de uppgifter som

[39] GDPR. Artikel 6.1c.
[40] Datainspektionen. *Rättslig förpliktelse*.
[41] GDPR. Artikel 6.1d.
[42] Datainspektionen. *Skydda grundläggande intressen*.
[43] GDPR. Artikel 6.1e.
[44] Datainspektionen. *Uppgift av allmänt intresse och myndighetsutövning.*
[45] GDPR. Artikel 6.1f.
[46] GDPR. Skäl 47.
[47] GDPR. Artikel 12.

behandlas.[48] Den registrerade har även rätt att få bekräftelse från den personuppgiftsansvarige om uppgifter som rör denne håller på att behandlas.[49]

- *Rättelse och radering*

Den registrerade har rätt till att få felaktiga personuppgifter rättade utan onödigt dröjsmål.[50] Vidare har den registrerade rätt till att utan onödigt dröjsmål få uppgifter raderade. Raderandet gäller även för uppgifter som inte längre är nödvändiga för det i förväg bestämda ändamålet, eller om den registrerade dragit tillbaka sitt samtycke.[51] Den registrerade har rätt att få behandlingen av personuppgifterna begränsade, exempelvis om den registrerade inte vill helt radera uppgifterna utan bara begränsa uppgifterna.[52] Vid rättelse eller radering ska den personuppgiftsansvarige även underrätta alla mottagare som de levererat personuppgifter till om det inte medför oproportionerlig ansträngning.[53]

Dataportabilitet är en stor nyhet med GDPR. Detta innebär att den registrerade har rätt att få ut de registrerade personuppgifterna på ett strukturerat sätt för att sedan kunna överföra dessa uppgifter till en annan personuppgiftsansvarig. Denna rätt kan också innebära att om det finns tekniska möjligheter ska den ursprungliga personuppgiftsansvariga skicka uppgifterna direkt till den nya personuppgiftsansvariga.[54]

- *Rätt att göra invändning och automatiserade individuella beslutsfattande*

Den registrerade har rätt till att när som helst göra invändningar om det finns skäl för det mot behandlingen av personuppgifter som berör den registrerade och som den registrerade inte har samtyckt till. Den personuppgiftsansvarige får då inte längre behandla uppgifterna utifall att den personuppgiftsansvarige inte kan påvisa skäl som väger tyngre än den registrerades intressen.[55]

Den registrerade besitter rätt att inte bli föremål för ett beslut som fattats enbart via automatiserad behandling.[56] Detta innebär att den registrerade har rätt att inte få ett beslut enbart genom automatiserad behandling som kan ha rättsliga följder som i hög grad påverkar den registrerade. Exempel kan vara ett avslag på en e-rekrytering utan någon personlig kontakt.[57]

2.7 Ansvarsrollerna

Ett av syftena i GDPR är att tydligt klargöra vad de olika rollerna som behandlar personuppgifter har för ansvar och skyldigheter.[58]

[48] GDPR. Artikel 13, artikel 14.
[49] GDPR. Artikel 15.
[50] GDPR. Artikel 16.
[51] GDPR. Artikel 17.
[52] GDPR. Artikel 18.
[53] GDPR. Artikel 19.
[54] GDPR. Artikel 20.
[55] GDPR. Artikel 21.
[56] GDPR. Artikel 22.
[57] GDPR. Skäl 71.
[58] GDPR. Skäl 11.

- *Personuppgiftsansvarig*

Detta ansvar kan bäras av en fysisk person, juridisk person, offentlig myndighet eller institution som ensamt eller i samråd med andra bestämmer syftet och med vilka medel som personuppgifter behandlas.[59] Om det är flera som är personuppgiftsansvariga ska de under öppna former fastställa sina respektive ansvar för att fullgöra sina skyldigheter enligt förordningen. Det föreligger ett solidariskt ansvar dem emellan.[60] En personuppgiftsansvarig ska föra register över behandlingen som sker under dennes ansvar som ska innehålla kontaktuppgifter, ändamålsbeskrivning för behandlingen, kategorisering av registrerade och av personuppgifter.[61] Denne har även ansvar att utifrån bland annat behandlingens art, omfattning och risker se till att genomföra tekniska och organisatoriska åtgärder för att garantera att behandlingen sker i enlighet med förordningen.[62] De har även ansvar för att det finns ett lämpligt dataskydd för behandlingen om det krävs utifrån uppgifternas innehåll.[63] I och med GDPR ska det göras en konsekvensbedömning för personuppgiftsbehandling med hög risk. Detta ska göras för att identifiera risker, sannolikheter för att riskerna ska inträffa och vad det kan ge för konsekvenser och följder för de registrerade.[64] Om konsekvensbedömningen visar på hög risk som inte genom lämpliga åtgärder kan begränsas ska den personuppgiftsansvarige samråda med Datainspektionen innan behandlingen påbörjas.[65] De ska även kunna påvisa att de använder godkända uppförandekoder eller certifieringsmekanismer och att dessa efterlevs.[66]

- *Personuppgiftsbiträde*

Personuppgiftsbiträde är en fysisk eller en juridisk person som för den personuppgiftsansvariges räkning behandlar personuppgifter.[67] Enligt PUL hade personuppgiftsbiträdet inga specifika skyldigheter vad det gäller själva behandlingen, men detta ändras med GDPR. Detta kommer bland annat innebära att de måste upprätta registerbeskrivningar och säkerställa lämplig säkerhetsnivå.[68] En personuppgiftsansvarig kan inte delegera sitt ansvar helt och hållet till biträdet, utan denne ska behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige. Hur hanteringen sker ska regleras i ett biträdesavtal där det framgår vilka som ska behandlas, hur länge det ska behandlas, arten och för vilket ändamål. Om denne behandlar uppgifterna på ett sådant sätt att det ses som för egen vinning, eller utöver biträdesavtalet, kan biträdet istället ses som personuppgiftsansvarig för dessa uppgifter.[69]

- *Dataskyddsombud*

Många företag och organisationer som behandlar personuppgifter i en stor omfattning eller behandlar känsliga uppgifter kommer behöva utse ett dataskyddsombud.[70] Dennes huvudsakliga uppgift kommer vara att informera och rådgiva organisationen om sådana skyldigheter som

[59] GDPR. Artikel 4.7.
[60] GDPR. Artikel 26.1.
[61] GDPR. Artikel 30, skäl 82.
[62] GDPR. Artikel 24.1.
[63] GDPR. Artikel 26.1.
[64] GDPR. Artikel 35.
[65] GDPR. Artikel 36.
[66] GDPR. Artikel 24.3.
[67] GDPR. Artikel 4.8.
[68] GDPR. Artikel 30.2, artikel 28.3c.
[69] GDPR. Artikel 28.
[70] GDPR. Artikel 37.

följer av förordningen. Ombudet ska även kontrollera att skyldigheterna följs och ska vara Datainspektionens kontaktperson.[71] De yrkesmässiga kvalifikationskraven som ställs på ett dataskyddsombud enligt GDPR är sakkunskap om lagstiftning och praxis avseende dataskydd samt förmåga att kunna fullgöra de angivna uppgifterna.[72] Dataskyddsombudet ska ha en oberoende ställning gentemot personuppgiftsansvarig och personuppgiftsbiträdet.[73]

2.8 Överföring till tredjeland

När personuppgifter förs över från ett EU land till ett land som inte ingår i EU eller EES så kallas detta för en överföring till tredjeland.[74] Detta aktualiseras exempelvis vid tillfällen då ett dokument med personuppgifter skickas via mail till ett tredjeland, eller när företag sparar personuppgifter på en server/molntjänst som finns i ett tredjeland.[75] Sådana här typer av överföringar är endast tillåtna i vissa specifika fall som finns uppställda i GDPR. Denna regel är till för att skydda personuppgifter då det inte finns liknande generella regler utanför EU. Situationer där GDPR godkänner tredjelandsöverföring är;

- Om EU-kommissionen har givit ett beslut att ett visst land kan säkerställa adekvat skyddsnivå.[76]

- Om ett sådant beslut som nämnt ovan fattas kan en överföring ske om lämpliga skyddsåtgärder vidtagits.[77] Med lämpliga skyddsåtgärder menas exempelvis att standardavtalsklausuler som EU-kommissionen har beslut om använts, dessa innehåller skyldigheter för den personuppgiftsansvariga/personuppgiftsbiträdet och för den som tar emot uppgifterna. Det kan även vara genom att använda bindande företagsbestämmelser. Bindande företagsbestämmelser är regler som sätts upp för företagets personuppgiftshantering och som har godkänts av en tillsynsmyndighet i EU. Eller genom att använda godkända uppförandekoder eller certifieringsmekanismer.[78]

- Om det inte föreligger något beslut om adekvat skyddsnivå eller att det finns några lämpliga skyddsåtgärder, så får överföringen endast ske i vissa specifika fall. Såsom om den registrerade uttryckligen samtyckt till överföringen efter att ha blivit informerad om riskerna. Eller om överföringen är nödvändig för att fullgöra ett avtal mellan den personuppgiftsansvarige och den registrerade eller annan fysisk/juridisk person för den registrerades intresse. Samt fall där överföringen är nödvändig för skäl som rör det allmänna intresset.[79]

2.9 Vid händelse av en personuppgiftsincident

En annan stor och viktig nyhet i GDPR är anmälan av personuppgiftsincidenter. Detta har helt och hållet saknats i PUL. De nya reglerna har som syfte att skydda personer från skada så som

[71] GDPR. Artikel 39.
[72] GDPR. Artikel 37.5.
[73] GDPR. Artikel 38.3.
[74] Datainspektionen. *Överföring till tredje land*.
[75] Datainspektionen. *Vad menas med överföring till tredje land?*.
[76] GDPR. Artikel 45.
[77] GDPR. Artikel 46.1.
[78] Datainspektionen. *Hur vidtar vi lämpliga skyddsåtgärder?*.
[79] Datainspektionen. *Hur vidtar vi lämpliga skyddsåtgärder?*.

att förlora kontrollen över sina personuppgifter, begränsning av deras rättigheter, diskriminering, identitetsstöld, risk för bedrägerier, ekonomisk förlust, skadat anseende, förlust av konfidentialitet för personuppgifter som omfattas av tystnadsplikt.[80]

Personuppgiftsincident beskrivs i GDPR som en säkerhetsincident som leder till en oavsiktlig eller olaglig förstöring, förlust, ändring eller till obehörigt röjande eller åtkomst av de personuppgifter som har behandlats.[81]

Om en personuppgiftsincident skulle inträffa ska den personuppgiftsansvarige så snart som möjligt och utan onödigt dröjsmål anmäla incidenten till Datainspektionen. Detta får inte ske senare än 72 timmar efter att den personuppgiftsansvarige har fått vetskap om incidenten. Personuppgiftsbiträden har som ansvar att rapportera incidenter till den personuppgiftsansvarige utan onödigt dröjsmål.[82] En anmälan behöver inte upprättas om det är osannolikt att en personuppgiftsincident skulle medföra skada för de registrerade.[83] En anmälan till Datainspektionen ska åtminstone bestå av personuppgiftsincidentens art, kategorier av och antal registrerade som berörs, samt kategorier och antal personuppgiftsposter som berörs. Den ska även innehålla kontaktuppgifter till dataskyddsombudet eller andra kontakter som kan erhålla mer information. Den ska dessutom innehålla sannolika konsekvenser av incidenten och beskrivande åtgärder som den personuppgiftsansvarige vidtagit eller föreslagit för att mildra de negativa effekterna. Den personuppgiftsansvarige ska föra dokumentation över alla personuppgiftsincidenter som skett, omständigheter kring dessa, effekter och åtgärder som vidtagits. Denna dokumentation ska föras för att möjliggöra Datainspektionens efterlevnadskontroll.[84]

En anmälan till den berörda registrerade ska ske om det sannolikt kommer medföra en hög risk för den fysiska personens rättigheter och friheter så att personen kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse ska ske så snart det är möjligt.[85] Anmälan ska innehålla en tydlig beskrivning av incidenten, kontaktuppgifter till dataskyddsombud, sannolika konsekvenser samt beskriva åtgärder. Den registrerade behöver ej informeras om det har vidtagits skyddsåtgärder, exempelvis kryptering så att obehöriga ej kan läsa uppgifterna, eller om det har vidtagits åtgärder som gör att det inte längre finns en hög risk för skada, eller om det skulle vara en oproportionerlig ansträngning. Vid det sista uppräknade fallet kan det istället ges ut information till allmänheten så att de berörda ändå får information om det inträffade.[86]

Exempel på personuppgiftsincidenter är när företaget råkat ut för dataintrång där registrerade uppgifter över de anställda finns. Ett annat exempel kan vara när personuppgifter mailats till fel mottagare som därmed får tillgång till känsliga uppgifter som den personen inte har behörighet till.[87]

[80] GDPR. Skäl 85.
[81] GDPR. Artikel 3.12.
[82] GDPR. Artikel 32.2.
[83] GDPR. Skäl 85.
[84] GDPR. Artikel 33.
[85] GDPR. Skäl 86.
[86] GDPR. Artikel 34.
[87] Datainspektionen. *När ska vi informera de registrerade?*.

2.10 Övervakningen och sanktionerna

Om den registrerade lidit materiell eller immateriell skada till följd av överträdelse av förordningen har denne rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet. Skadeståndsskyldigheten gäller dock ej om det kan påvisas att de inte på något sätt är ansvariga för skadan. Begreppet skada ska tolkas brett mot bakgrund av rättspraxis.[88]

Datainspektionen har fått ett större ansvar och många fler uppgifter i och med förordningen. De ska utöva tillsyn för att se till att förordningen följs och ansvarar för att säkerställa att de administrativa sanktionsavgifterna ska verka effektivt, avskräckande och i proportion. Datainspektionen ska i varje enskilt fall ta hänsyn till de olika omständigheterna så som överträdelsens karaktär, svårighetsgrad, om överträdelsen skett uppsåtligt eller genom oaktsamhet, tidigare överträdelser, åtgärder som vidtagits och graden av samarbete med Datainspektionen. Administrativa sanktionsavgifter kan uppgå till ett belopp av 20 000 000 euro eller upp till 4% av företagets totala globala årsomsättning.[89]

2.11 GDPR:s undantag för småföretag

GDPR har inte några direkta undantag för småföretagare, förutom angående den personuppgiftsansvariges registeransvar som nämndes i avsnitt 2.7. Ett sådant register behöver ej föras om organisationen sysselsätter färre än 250 personer såvida behandlingen ej kommer medföra en risk för registrerades rättigheter och friheter.[90] Detta innebär därmed att småföretagen lyder under lika tunga krav som stora företag beträffande behandling, åtgärder och sanktioner.

[88] GDPR. Artikel 82, skäl 146.
[89] GDPR. Artikel 83.
[90] GDPR. Artikel 30.5.

3. De stora skillnaderna mellan GDPR och PUL

I följande kapitel kommer de grundläggande skillnaderna mellan GDPR och PUL presenteras mer ingående med utgångspunkt i respektive lagtext.

3.1 Tillämpningsområdet

När GDPR träder i kraft kommer en viktig regel som funnits i PUL tas bort, den så kallade missbruksregeln. PUL har delat in material i två olika kategorier, strukturerat material och ostrukturerat material. Exempel på vad som utgör strukturerat material enligt PUL är uppgifter i register och databaser. Med ostrukturerat material menas enligt PUL personuppgifter som förekommer i exempelvis löpande text, mailkonversationer, publicering av personuppgifter på webbplatsen och bilder.[91] Missbruksregeln har inneburit att ostrukturerat material inte behöver behandlas i enlighet med PUL så länge det inte missbrukas och kränker den personliga integriteten.[92] Missbruksregelns syfte har inneburit en lättnad för vardaglig ostrukturerad behandling av personuppgifter.[93]

En annan stor skillnad är det territoriella tillämpningsområdet. I PUL 4§ beskrivs att lagen endast gäller de personuppgiftsansvariga som är etablerade i Sverige, eller om den personuppgiftsansvarige är etablerad i tredjeland men behandlingen utförs genom utrustning som är lokaliserad i Sverige. Genom artikel 3 i GDPR förändras det territoriella tillämpningsområdet radikalt. GDPR ska tillämpas oavsett vilket land inom EU som den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerat i och oavsett om behandlingen sker inom unionen eller inte. Vidare gäller även att förordningen ska tillämpas om personuppgifterna tillhör en medborgare inom unionen men behandlingen sker i ett tredjeland om behandlingen har anknytning till utbjudande av varor eller tjänster till registrerade i EU eller övervakning av beteende inom unionen. Detta innebär alltså att alla företag som är stationerade utanför EU men med kunder inom EU nu blir berörda av förordningen.

3.2 Principer för behandling

De principer som ska följas vid personuppgiftsbehandling enligt GDPR artikel 5 återfinns med benämningen ”krav på behandlingen” i PUL i 9§. En skillnad är att i GDPR artikel 5 punkt 1a har lagts till att behandlingen ska ske på ett öppet sätt vilket hänvisar till att det ska för den registrerade vara klart och tydligt hur uppgifterna behandlas.[94] Den andra förhållandevis stora skillnaden är tillägget med principen ansvarsskyldighet. Denna princip ger den personuppgiftsansvarige ansvaret över att personuppgiftsbehandlingen följer de uppställda principerna, samt kunna visa för datainspektionen att och hur principerna följs. Den personuppgiftsansvarige ska kunna bevisa att lämpliga tekniska och organisatoriska åtgärder har genomförts samt att dessa åtgärder ses över och uppdateras vid behov. Åtgärdernas effektivitet måste också kunna visas.[95]

3.3 Rättslig grund för behandling

De rättsliga grunder som utgör om behandlingen är laglig överensstämmer väl i GDPR artikel 6 och PUL 10§. Skillnaden är att GDPR ställer upp villkor för samtycken i artikel 7. Bland dessa villkor pekas den personuppgiftsansvarige ut som bärare av bevisbördan att ett samtycke förekommer. Det finns även ett tillägg bland villkoren som rör samtycken som lämnas skriftligt

[91] Datainspektionen. *Strukturerat eller ostrukturerat?*.
[92] PUL. 5a§.
[93] Datainspektionen. *Strukturerat eller ostrukturerat?*.
[94] Datainspektionen. *Dataskyddsförordningens grundläggande principer.*
[95] GDPR. Skäl 74.

tillsammans med text som rör andra frågor, samtycket ska då kunna utskiljas på ett klart och tydligt sätt, ifall detta ej görs kommer det att resultera i att samtycket ej är bindande. Detta aktualiseras exempelvis när den registrerade erhåller en längre avtalstext. Både i PUL 12§ och i villkoren i artikel 7 punkt 3 i GDPR har den registrerade rätt att återkalla ett samtycke. Det som skiljer sig nämnvärt här är att enligt GDPR så ska den registrerade bli informerad om återkallning av samtycke vid tillfället då samtycket ges samt att GDPR utrycker att det ska vara enkelt att återkalla ett samtycke, lika enkelt som att samtycka.

3.4 Den registrerades rättigheter

GDPR innebär en stor del utökade rättigheter för de registrerade vilket resulterar i att som registrerad har större kontroll över sina uppgifter. Dessa är som nämnt tidigare uppdelad i olika avsnitt i GDPR. Det första avsnittet rör insyn och villkor. Det som främst skiljer sig här är att GDPR i artikel 12 uttryckligen betonar vikten av att all information och kommunikation ska ske på ett klart, tydligt, lättförståeligt sätt och i en lättillgänglig form vilket inte återfinns i PUL. Det finns även en skillnad i att den personuppgiftsansvarige ska enligt GDPR artikel 12 punkt 3 efter en begäran från den registrerade om information som rör personuppgiftsbehandlingen erhålla denne detta utan onödigt dröjsmål och senast inom en månad. Detta får även förlängas med två månader om begäran är komplicerad eller på grund av att det inkommit ett flertal begäran. Enligt PUL 26§ är istället den personuppgiftsansvarige skyldig att lämna ut sådan information en gång per år och den informationen ska lämnas inom en månad men beroende på begäran och antal inkomna begäran ska det maximalt ta 4 månader.

Det andra avsnittet berör information och tillgång till personuppgifterna. Den mest betydande skillnaden här är att GDPR i artikel 13–15 utökar den information som ska utges, bland annat så ska informationen alltid innehålla förekomsten av rätten att begära rättelse eller radering och under vilket tidsperiod uppgifterna kommer lagras.

Det tredje avsnittet rör rättelse och radering. Rättelse som återfinns i artikel 16 i GDPR och i PUL 28§ är i stort sätt den samma. Den stora skillnaden är istället att med GDPR kommer en klausul som ger individer ”rätten att bli bortglömd”, detta återfinns i artikel 17. Detta innebär att den registrerade kommer bära rätten att utan onödigt dröjsmål få uppgifter raderade samt att företagen själva måste radera uppgifter som inte längre är nödvändiga för de ändamålet som de från början samlades in för. Utöver rätten till radering har den registrerade med GDPR rätt att begränsa behandlingen av personuppgifterna enligt artikel 18 och den registrerade har även rätt till dataportabilitet enligt artikel 20.

Det fjärde avsnittet berör rätten att göra invändningar samt automatiserade beslutsfattande, regleringar för de automatiserade beslutsfattandet är i stort sätt oförändrad.[96] Däremot är Invändningsrätten som återfinns i artikel 21 är en nyhet i och med GDPR. Denna rätt innebär att den registrerade får när som helst invända mot behandlingen av personuppgifter som den registrerade inte har samtyckt till.

3.5 Ansvarsrollerna

Den personuppgiftsansvariges ansvarsroll är i stort sett oförändrat med GDPR då båda beskriver att denna är ytterst ansvarig för att reglerna för personuppgiftsbehandling följs.[97] Den förändring som är störst är att personuppgiftsbiträdets skyldigheter ökar. Enligt PUL 31§ så är det

[96] GDPR. Artikel 22. PUL. 29§.
[97] GDPR Artikel 21.1. PUL. 9§, 31§.

den personuppgiftsansvarige som ska genom ett avtal dem emellan reglera vilka typer av säkerhetsåtgärder som biträdet måste vidta samt förvissa sig om att de verkligen har vidtagits. Medan GDPR istället genom artikel 28 punkt 3c pekar ut att det är personuppgiftsbiträdet ansvar att se till att artikel 32 följs som beskriver att lämpliga tekniska och organisatoriska åtgärder samt garantera en lämplig säkerhetsnivå i förhållande till riskerna.

Med GDPR tillkommer nya ansvarsområden, dessa är de som behandlas i artikel 33-36 och rör anmälan av personuppgiftsincident samt konsekvensbedömning vid personuppgiftsbehandling (se nedan avsnitt 3.7 samt 3.8), dessa nya ansvarsområden tillfaller den personuppgifts-ansvarige och personuppgiftsbiträdet om en sådan används.

Dataskyddsombud är det nya namnet på ett personuppgiftsombud, förutom namnbytet så har denna roll som tidigare enligt PUL varit frivillig nu blivit en skyldighet för vissa företag och organisationer att utse. Detta gäller förutom myndigheter och andra offentliga organ som behandlar personuppgifter även företag som behandlar personuppgifter i stor utsträckning samt om känsliga uppgifter behandlas enligt artikel 37 i GDPR. Dataskyddsombudets arbetsuppgifter samt ansvarsområden är i princip de samma i PUL och GDPR.[98]

3.6 Säkerheten och inbyggt dataskydd

I GDPR artikel 25 finns en regel om dataskydd. Denna regel har ingen motsvarighet i PUL. Den kräver att företag vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personers rättigheter och friheter i samband med personuppgiftsbehandling. Den omfattar uppgiftsminimering, pseudonymisering av personuppgifter, minimering av lagringstid samt minimering av tillgänglighet.

3.7 Konsekvensbedömning

Konsekvensbedömning är något som måste utföras om behandlingen kan innebära stora risker enligt artikel 35 i GDPR. Bedömningen ska innehålla behandlingens syfte, risker samt hur dessa risker hanteras. Om det i konsekvensbedömningen framkommer att det föreligger hög risk med behandlingen måste ett samråd med tillsynsmyndigheten ske för att komma fram till eventuella åtgärder för att minimera denna risk enligt artikel 36.

3.8 Personuppgiftsincident

I enlighet med artikel 33 i GDPR kommer den personuppgiftsansvarige att ha en rapporteringsskyldighet vid personuppgiftsincidenter. Denna rapportering ska ske inom 72 timmar till datainspektionen. Om incidenten är allvarlig och kan innebära en hög risk för den registrerades rättigheter och friheter ska även den registrerade underrättas enligt artikel 34.

3.9 Övervakning och sanktionerna

Det blir i GDPR fastställt i lagen enligt artikel 77 att registrerade har möjlighet att lämna klagomål till datainspektionen. Detta är ett nytt tillägg då det inte funnits uttryckt i PUL att den registrerade bär denna rättighet. Detta ska kunna göras om den registrerade anser att behandlingen av dennes personuppgifter är felaktig eller bryter mot förordningen. PUL beskriver att enligt 48§ så ska den personuppgiftsansvarige ansvara för skada och kränkningar av den personliga integriteten. GDPR beskriver istället att en person som lidit materiell eller immateriell skada på grund av överträdelsen har rätt till ersättning från personuppgiftsansvarige eller från

[98] GDPR. Artikel 39. PUL. 38§.

personuppgiftsbiträdet enligt artikel 82 punkt 1. Detta innebär alltså att även biträdet kan bli skadeståndsskyldig.

Brott mot PUL genom uppsåt eller grov oaktsamhet kan enligt PUL 49§ dömas till böter eller fängelse i högst sex månader och om brottet är grovt till fängelse högst två år. Enligt PUL ska datainspektionen först genom påpekande få till en rättelse vid olovlig personuppgiftsbehandling och om rättelse ej sker kan datainspektionen utdöma vite.[99] Enligt artikel 83 i GDPR kan sanktionsavgifter dömas direkt efter tillsynen av datainspektionen efter upptäckta brister om överträdelsen skett med uppsåt eller genom grov oaktsamhet. Dessa sanktionsavgifter kan uppgå till 20 000 000 euro eller upp till 4% av företagets globala årsomsättning. GDPR sanktioner och viten är betydligt strängare än i PUL. Verksamheter kan alltså på grund av GDPR komma att lida stora ekonomiska förluster till följd av överträdelser.

[99] PUL. 43–49§§.

4. Småföretagens genomförande

I detta kapitel presenteras konkreta exempel när personuppgifter hanteras i ett företag för att kort exemplifiera situationer som lagstiftningen behandlar. Sedan förklaras de främsta åtgärder som företag behöver göra för att anpassa sig till den nya lagstiftningen.

4.1 Situationer där företag hanterar personuppgifter

4.1.1 Företags hantering av personuppgifter vid kundförhållande

Som beskrivits i kapitel två är alla uppgifter som kan knytas an till en fysisk levande person en personuppgift och när personuppgifter behandlas genom helt eller delvis automatisk behandling eller genom ett manuellt register ska detta ske i enlighet med förordningen. Många företag för kundregister med personuppgifter, vid dessa fall måste kunden bli informerad om vilka typer av uppgifter som sparats. om uppgifterna som sparas anses vara mer än vad som egentligen behövs för att verkställa ett avtal måste kunderna ha gett sitt samtycke. Detsamma gäller för bokningssystem, om exempelvis kundens preferenser har antecknats vid en tidigare bokning så är det att anses som mer uppgifter än vad som är berättigat för att uppfylla ett avtal och måste därför först godkännas av kunden. Vissa företag använder sig av mailkorrespondens, de måste då ta i beaktan att det aldrig skickas känsliga uppgifter via mail och det måste skapas rutiner för att kontinuerligt radera mail med personuppgifter.[100]

4.1.2 Företags hantering av personuppgifter vid leverantörsförhållande

Företag hanterar uppgifter som rör deras leverantörer. Leverantörsregister innehåller dock oftast juridiska personer och dessa berörs inte av GDPR. Men om uppgifterna berör enskilda näringsidkare eller exempelvis en kontaktperson hos leverantörerna är detta en personuppgift och ska hanteras i enlighet med förordningen. Som exempel kan nämnas att om ett företag avslutar ett samarbete med en leverantör så ska personuppgifter som rör denne raderas då de inte längre tjänar något syfte.[101]

4.1.3 Företags hantering av personuppgifter vid anställningsförhållande

GDPR gäller för all behandling av personuppgifter, således måste även behandling av uppgifter om anställda utföras på ett lagligt och korrekt sätt. Ändamål måste bestämmas innan behandling och de får inte vara för allmänt hållna. Uppgifterna måste vara adekvata och relevanta för ändamålet av behandlingen, alltså ska inte mer uppgifter registreras än vad som behövs. Uppgifter som inte längre är aktuella ska tas bort, exempelvis när en anställning avslutas.

En arbetsgivare måste informera de anställda om vilka uppgifter som finns insamlade och vad de ska användas till. Om arbetsgivaren samlat in uppgifter från en annan källa än från den anställda ska även dessa uppgifter informeras.

För att insamlingen ska vara laglig krävs rättslig grund, antingen via samtycke eller någon av de andra grunder som räknas upp i förordningen. Insamlingen får ske om det är nödvändigt för att anställningsavtalet ska kunna uppfyllas, exempelvis personaladministrativa system som löneberäkning eller sjukfrånvaroregistrering eller in- och utpasseringssystem. En annan rättslig grund är om registreringen är en rättslig skyldighet exempelvis för redovisning av skatter och sociala avgifter. Intresseavvägning kan användas som rättslig grund vid exempel registrering av anhörigas kontaktuppgifter om det skulle inträffa en sjukdom eller olycksfall. Här behövs

[100] Verksamt. *GDPR-guiden.*
[101] Verksamt. *GDPR-guiden.*

inget samtycke från de anhöriga men de måste ändå blivit informerade om att uppgifterna finns lagrade.

En stor skillnad för arbetsgivare kommer att bli att de uppgifter som har behandlats i ostrukturerat material nu måste behandlas enligt GDPR. Särskilt kommer detta innebära att samtycke måste samlas in för material som finns på företagets hemsida så som publicerade namn på anställda, befattning, telefonnummer, e-postadress och bilder på anställda.[102]

4.2 Anpassningsarbetet inför GDPR

Företagens GDPR-anpassning kommer att innebära många åtaganden, främst ligger det stor vikt vid att alla delar av företagen sätter sig in i samt bildar sig en uppfattning om den nya regleringen. Ledningen och de som hanterar personuppgifter i företagen måste vara väl insatta i GDPR. Företagen måste identifiera vilka typer av information som de hanterar och om det omfattas av den nya lagen. De måste säkerställa vilka i företagen som bär de olika roller och vad deras ansvar innebär samt se till att de kontinuerligt arbetar med sina ansvarsområden.[103]

Företag bör se till att det förs dokumentation av olika slag så som vilka typer av personuppgifter hanteras, hur har de samlats in och till vem lämnas uppgifterna ut till.[104] Den personuppgiftsansvariges ansvar kommer genom ansvarsskyldigheten öka och denne måste kunna visa att reglerna följs och hur företagets behandling av personuppgifter är laglig.[105] Det bör också föras dokumentation över den rättsliga grunden, exempelvis för att kunna visa att det finns ett samtycke för behandlingen.[106]

Företag måste se över hur de informerar de registrerade vid insamling av uppgifter i och med att personuppgiftsansvariga har fått ett utökat informationskrav till den registrerade. Detta innebär att det tydligt ska framgå den personuppgiftsansvariges identitet, ändamål med behandling, rättslig grund för behandling, hur länge uppgifterna kommer lagras samt om möjligheten för den registrerade att lämna in klagomål till Datainspektionen.[107]

Många företag måste göra stora åtgärder vad gäller dataskydd i samtliga delar av företaget där personuppgifter behandlas, medarbetare måste utbildas i hur det på ett säkert sätt behandlar personuppgifter och i vissa fall måste ett dataskyddsombud tillsättas. Ett dataskydd måste finnas inbyggt i företagens IT-system, det måste således undersökas om de befintliga systemen uppnår GDPR:s krav.[108] Företaget måste se till att de inte samlar in mer information än vad som behövs, att informationen inte lagras längre än för det ursprungliga syftet.[109] Företag måste se till att det finns möjligheter för den registrerade att få ut information som finns lagrad om denne[110] samt ha rutiner för dataportabilitet.[111]

---

[102] Verksamt. *GDPR-guiden.*
[103] Datainspektionen. *Förberedelser för personuppgiftsansvariga*.
[104] Datainspektionen. *Förberedelser för personuppgiftsansvariga*.
[105] GDPR. Artikel 5.2.
[106] Skäl 91. Datainspektionen. *Förberedelser för personuppgiftsansvariga*.
[107] GDPR. Artikel 13. Datainspektionen. *Förberedelser för personuppgiftsansvariga*.
[108] Datainspektionen. *Förberedelser för personuppgiftsansvariga*.
[109] GDPR. Artikel 25.
[110] GDPR. Artikel 15.
[111] GDPR. Artikel 20.

Missbruksregelns försvinnande kommer att innebära stora administrativa förändringar för företag som tidigare utnyttjat denna regel. Företag måste se till att även ostrukturerat material sköts i enlighet med GDPR, exempelvis klargöra förutsättningar som finns för behandlingen, om de har en rättslig grund för behandlingen, att det finns tillräckligt med tekniskt skydd för uppgifterna, och att de raderas när det inte längre behövs.[112]

Företag som hanterar personuppgifter som är förenade med risker för enskildas fri och rättigheter måste utföra en konsekvensbedömning, i vissa fall måste de även samråda med Datainspektionen om företaget hanterar personuppgifter som kan medföra höga integritetsrisker för de registrerade.[113]

Det ställs nya krav gällande rapportering av personuppgiftsincidenter. I och med kravet att en anmälan till Datainspektionen inte får ske senare än 72 timmar efter att den personuppgiftsansvarige har fått vetskap om incidenten är det viktigt att företag har tillräckliga rutiner för att upptäcka, rapportera och utreda incidenter för att leva upp till dessa regler. I och med att tiden för anmälan är kort måste företaget bestämma på förhand var ett sådant ansvar ligger så att anmälan kan ske inom tidsfristen.[114]

[112] Datainspektionen. *Förberedelser för personuppgiftsansvariga*.
[113] GDPR. Artikel 35, artikel 36.
[114] GDPR. Artikel 33. Datainspektionen. *Förberedelser för personuppgiftsansvariga*.

5. Undersökning om småföretag är förberedda inför GDPR

I följande kapitel presenteras först Vismas undersöknings utfall och därefter resultatet från min undersökning.

5.1 Vismas undersökning

Under mars månad (2 månader före GDPR) genomförde företaget Visma en undersökning nationellt bland sina kunder i gruppen småföretagare. De frågor som ställdes var:

- *Den 25 maj träder EU:s nya dataskyddsförordning GDPR i kraft. Har du satt dig in i vad de nya reglerna för skydd av personuppgifter innebär för ditt företag?*
- *Har du vidtagit några konkreta åtgärder i ditt företag med anledning av GDPR, till exempel GDPR-säkrat kundregistret eller raderat gamla personuppgifter om eventuella medarbetare?*

Det sammanställda resultatet visade att endast 44% hade satt sig in i de nya reglerna och vad det kommer betyda för företagets personuppgiftshantering. På fråga 2 svarade 13% att de har vidtagit konkreta åtgärder med anledning av GDPR.[115]

5.2 Min undersökning

Jag genomförde min undersökning under slutet av april (1 månad före GDPR) bland småföretag i Norrbotten. De frågor som ställdes var:

- *Har ni på (förtagets namn) satt er in i vad de nya reglerna innebär för ert företag?*
- *Om ja, har ni gjort några konkreta åtgärder med anledning av reglerna?*

Av de 26 stycken småföretagare som deltog svarade 17 stycken ”ja” på frågan ”Har ni på (företagets namn) satt dig in i vad de nya reglerna för skydd av personuppgifter innebär för ert företag?”. Detta innebär alltså att 65% har satt sig in i vad de nya reglerna kommer att innebära för deras verksamhet. På samma fråga svarade 9 stycken ”nej”, vilket betyder att 35% fortfarande inte hade analyserat hur de påverkas av GDPR.

Den andra frågan ”om ja, har ni gjort några konkreta åtgärder med anledning av reglerna?”, som endast berör de som svarat ”ja” på första frågan, svarade totalt 11 stycken ”ja”. Det innebär att 42% av alla studiedeltagare har gjort konkreta förändringar. Om omfånget begränsas till den svarsgrupp som svarat ”ja” på den första frågan, det vill säga till 17 studiedeltagare så innebär det att 65% av de som satt sig in i de nya reglerna också har gjort konkreta förändringar. Genom att 6 stycken svarade ”nej”, har alltså 35% satt sig in i de nya reglerna men ännu inte gjort några förändringar vid frågetillfället.

[115] Mynewsdesk. *Två månader kvar: Bara fyra av tio småföretagare har satt sig in i GDPR.*

6. Analys och Diskussion

I detta kapitel diskuteras inledningsvis den första och den andra frågeställningen tillsammans då de sammanfaller något vid en analys. I sista delen diskuteras resultaten från undersökningarna.

6.1 Behandling av personuppgifter efter GDPR: hur kan företagen arbeta?

Den nya Dataskyddsförordningen är ett gediget arbete på 119 sidor med 99 artiklar och 173 skäl.[116] Det främsta syftet har varit att säkerställa enskildas rätt till sina personuppgifter, att harmonisera regleringar i EU för behandling av personuppgifter samt att komma i kapp med regler som överensstämmer med den tid vi nu lever i.

För att förbereda sig inför de stora förändringar som GDPR innebär, är det viktigt att i tid sätta sig in de nya regleringarna. Anpassning tar tid. För att kunna få en full förståelse är det viktigt att alla i ett företag blir insatta i de nya reglerna och gör en inventering kring vilka uppgifter som hanteras och hur de ska hanteras så det sker i enlighet med den nya förordningen. GDPR är en förhållandevis detaljerad och lättförståelig lagstiftning men den måste ändå analyseras noggrant.

I och med att personuppgiftsansvarige, personuppgiftebiträdet och dataskyddsombudet får nya och utökade ansvarsområden med nya skyldigheter är det viktigt att de blir införstådda med de nya kraven så att de från början kan hantera sina uppgifter korrekt. Personuppgiftsbiträden som tidigare inte haft så många skyldigheter står inför utmaningen att anpassa sig efter det nya reglerna, detta kommer även resultera i att personuppgiftsansvariga kommer behöva arbeta om sina biträdesavtal för att säkerställa att lagen följs. Enligt PUL har det varit frivilligt att ha ett dataskyddsombud men detta byts nu ut till ett krav vilket kommer gör att de berörda företagen behöver anställa ytterligare en person som kan bära denna rollen, alternativt anlita en konsult eller om rollen kommer bäras av en redan anställd som kontinuerligt behöver erhålla utbildning eller andra resurser för att kunna genomföra uppdraget.

En behandling av personuppgifters laglighet avgörs främst om artikel 5 och 6 är uppfyllda. Trots benämningen ”principer” i artikel 5, så innehåller den krav som tillsammans med de rättsliga grunderna i artikel 6 måste vara uppfyllda. Artikel 5 avser frågan ”hur” en behandling får ske för att den ska vara laglig, medan artikel 6 handlar om ”om” en behandling får ske. Den första uppräknade principen, den som avser laglighet, korrekthet och öppenhet, blir en hänvisning till artikel 6 då den rättsliga grunden så som samtycke och uppräknade situationer där samtycke ej behövs utgör en laglighetsgrund. Den personuppgiftsansvariges ansvarsskyldighet innebär ett ökat ansvar i form av att se till att principerna följs samt kunna bevisa för Datainspektionen hur de följs.

Ett samtycke måste lämnas frivilligt och ska vara specifikt. Den registrerade måste ha lämnat detta genom uttalande eller handling. Det får inte vara ett tyst/passivt samtycke. Bevisbördan av att ett samtycke existerar har den personuppgiftsansvarige. Nyheten att samtycken ska vara enklare att förstå genom ett klart och tydligt språk kommer att få konsekvenser för många företag, många kommer behöva arbeta om sina avtal så att samtycke för personuppgiftsbehandling inte försvinner in i mängden i avtalstexten. Det blir också en utmaning för den personuppgiftsansvarige att vara tillräckligt specifik i sin beskrivning men samtidigt avväga detta med att vara generell för att inte begränsa sitt handlingsutrymme allt för mycket.

[116] GDPR.

Ett av förordningens bakomliggande syften, att stärka den registrerades rättigheter och ge den registrerade mer kontroll över sina personuppgifter, återfinns i kapitel 3 i förordningen. Artikel 12 utgör en portalparagraf som avser information och kommunikation mellan den personuppgiftsansvarige och den registrerade. Detta innebär också att den personuppgiftsansvarige ska underlätta för den registrerade att utöva sina rättigheter så som rätt till tillgång, rättelse och radering. I ett avtal måste det tydligt framgå syftet med de sparade personuppgifterna så därmed får det inte förekomma avtal med friskrivning där den enskilda samtycker till att företaget lagrar dennes uppgifter utan att få en fullständig förklaring till ändamålet med personuppgiftsbehandlingen. Enskildas rättigheter har också blivit stärkta genom rätten till registerutdrag samt dataportabilitet. Detta kommer innebära att företag måste ha rutiner för att snabbt och korrekt kunna ta hand om sådana ansökningar.

Sverige har haft en undantagsregel i PUL när det gäller personuppgiftsbehandling, den så kallade missbruksregeln. Med GDPR kommer ostrukturerat material också vara tvunget att följa förordningen och detta kommer att få stora betydelser för företag som behandlat personuppgifter på detta sätt. Det måste ske lagligt, med en rättslig grund och den registrerade måste få information om behandlingen på ett korrekt sätt. Det måste även finnas rutiner för att skydda uppgifterna samt att radera dem när de inte längre är aktuella. Frågan som kan ställas är om det egentligen finns motiverad anledning till att allt material som är personuppgifter ska hanteras på samma sätt. Uppgifter som är föremål för vardagliga bestyr och som inte är att anse som riskfyllda tjänar mycket administrationstid på att få behandlas enligt missbruksregeln i PUL. Här måste dock poängteras att GDPR främsta syfte är att skydda den personliga integriteten och inte att effektivisera tillvägagångsättet för personuppgiftsbehandling.

Det har inte funnits regler i PUL om anmälan vid personuppgiftsincidenter. Konsekvenserna av detta nya anmälningskrav är att personuppgiftsansvariga behöver ha rutiner för att snabbt kunna identifiera vilka som berörts och bedöma risker för de registrerade. Detta ska meddelas till Datainspektionen och ska även i vissa fall informeras till de registrerade.

Tidigare har det varit ett fåtal som blivit bötfällda för brott mot PUL och därmed har lagen inte alltid tagits på så stort allvar,[117] men med GDPR finns det starka incitament för de som behandlar personuppgifter att ta dataskyddsfrågor på allvar. Företag riskerar höga sanktioner om de inte efterlever reglerna. Detta måste samtidigt innebära ett större arbete för Datainspektionen som med förordningen får ett utökat uppdrag.

Förordningen innehåller en del diffusa begrepp utan att riktigt beskriva innebörden. Exempelvis ska företag vidta ”lämpliga åtgärder” för att skydda personuppgifter. Om detta innebär kryptering eller att det finns en säker brandvägg är svårt att utläsa. Desamma gäller begreppet ”onödigt dröjsmål” som aktualiseras exempelvis vid radering om personuppgifter. Mer exakta förklaringar får inväntas från framtida prejudikat och praxis.

6.2 Är småföretagen i fas när det gäller anpassning inför de nya reglerna

Småföretagare är en särskilt utsatt grupp. Det är de med kanske minst möjligheter att bekanta sig med ny lagstiftning på grund av bristande kunskaper och resurser. Samtidigt utgör de en stor del av samhället och det är därför viktigt att de utför sitt arbete korrekt med tanke på risker för sanktioner, men också från registrerades synvinkel så att de ska känna sig säkra på att uppgifter de delar med sig av inte hanteras otillbörligt. Vismas undersökning visade resultatet att 44% av de som svarade hade satt sig in i de nya reglerna och endast 13% vidtagit konkreta

[117] Sveriges Radio. *Få fälls för misstänkta brott mot PUL*.

åtgärder. Tyvärr kan inte denna undersökning ge en rättvis bild av verkligheten med så låg svarsfrekvens som 5%. Undersökningen blir färgad av de som väljer att svara: det kan exempelvis vara så att de som känner sig bekanta med ordet GDPR väljer att svara eller sådana som känner sig osäkra men nyfikna som väljer att svara. Oavsett resultatet som Visma redovisar så kan det ändå utläsas att det finns företag som inte känner till förordningen och vad den innebär för deras företag. Det är bekymmersamt så nära inpå genomförandet.

Med min undersökning ville jag få en rättvisare bild på hur förberedda småföretagen är, dock ska ändå nämnas att 26 svarande inte heller kan uppfylla en korrekt verklighetsspeglig. Det som dock gör att den ändå får anses ge verklighetsbaserade indikationer är att jag har haft en hög svarsfrekvens. Min undersökning visar att 65% av de tillfrågade är insatta i de nya reglerna. Detta resultat visar att cirka 20% mer i min undersökning är införstådda i den nya lagen än vad Vismas tyder på. 65% är fortfarande ett lågt resultat med tanke på att dessa företag vid denna tidpunkt bara har 1 månad på sig att sätta sig in i reglerna innan de blir gällande rätt. Så gott som alla företag hanterar personuppgifter, om detta är i form av kunders uppgifter, leverantörers uppgifter eller om det bara består av uppgifter kring de anställda så behöver alla se över hanteringen. Företagen behöver veta vilka typer av uppgifter som hanteras, hur dessa hanteras och om det görs i enlighet med gällande rätt. Av de 26 företag som svarade på min undersökning svarade 42% att de vidtagit åtgärder på grund av GDPR. Av svarsgruppen som svarat ”ja” på första frågan svarade 65% av dem att de vidtagit åtgärder. Resultatet skulle kunna förklaras med att de företag som jag har varit i kontakt med inte behandlar så stora mängder av personuppgifter rörande deras kunder och därför inte känner sig träffade av GDPR, men oavsett detta så har alla företag jag kontaktade minst 10 anställda och behandlar således minst 10 anställdas personuppgifter. Detta är skäl nog att sätta sig in i reglerna för att se hur deras behandling kan påverkas av reglerna för att undvika sanktionskostnader.

GDPR för med sig många stora förändringar för behandling av personuppgifter. Trots det finns det bristande kunskap om de nya reglerna hos småföretagare. Det får anses bekymmersamt att så sent som 1 månad före genomförandet hade 35% inte satt sig in i vad de nya reglerna kommer innebära för deras företag. Av de 519 småföretag som fanns med på listan som jag gjorde mitt urval ifrån kan så många som 182 företag i Norrbotten riskera att få påföljder på grund av att de inte aktivt analyserat den nya lagstiftningen och hur den kommer påverka deras verksamhet.

6.3 Slutkommentar

Förordningens höga krav kommer innebära mycket anpassningsarbete och frågan är om detta är skäligt. Förordningen är till för att skydda enskilda men samtidigt så är det den enskilda som driver enmansföretag, mikrobolag och småföretag som utgör 99% av alla företag i Sverige som blir hårt drabbade.[118] Därtill har beräkningar visat att det kommer kosta europeiska företag 2 000 miljarder att anpassa sig till GDPR.[119] Det har dessutom visat sig att förordningen har förorsakat att företag lägger ned sina verksamheter inom Europa då anpassningsarbetet beräknas bli för kostsamt.[120] Förordningen har alltså visats minska utbudet inom Europa och sätta företagen i en utmanande ställning.

Då företag bevisligen har svårigheter att anpassa sig efter förordningen finns också möjligheten att Datainspektionen kommer ha svårigheter att kunna fullfölja sitt uppdrag. Det nya uppdraget innebär för verksamheten att de kommer få fler uppgifter som innebär stödjande och rådgivande

[118] Ekonomifakta. *Företagens storlek.*
[119] TT. *GDPR kommer att kosta 2 000 miljarder kronor*.
[120] Mölne, V. Dagens Industri. *Spelbolag stänger ner i Europa inför GDPR*.

för att hjälpa de som behandlar personuppgifter. De har även fler möjligheter och befogenheter att rapportera personuppgiftsincidenter, utöva tillsyn och utfärda sanktionsuppgifter. År 2018 har myndigheten erhållit 30 miljoner kronor för att stärka myndigheten och förhoppningsvis hjälpa myndigheten att kunna fullgöra sitt uppdrag.[121] Men i och med situationen som var tidigare att personuppgiftsbehandlare inte har tagit lagen på så stort allvar blir frågan om detta verkligen är tillräckligt för att se till att lagen efterlevs. Som min statistik visade, att så sent som 1 månad innan införandet var 35% fortfarande inte insatta i den nya lagen. Kommer företag räkna med att Datainspektionen inte kommer klara av det nya uppdraget, och kommer det då resultera i att GDPR precis som PUL inte respekteras fullt ut?

Inför framtiden skulle det vara intressant att följa upp och se hur statistiken ser ut efter genomförandet den 25 maj 2018. Har företag hunnit anpassa sig i tid? Det skulle också vara intressant att genomföra en undersökning för att försöka komma åt varför företag väljer att inte sätta sig in i regler som berör något så viktigt som den personliga integriteten.

[121] Eriksson, W. Dagens Juridik. *Datainspektionen blir Integritetsskyddsmyndigheten - får 30 miljoner för satsning på GDPR*.

Källor och litteratur

Offentligt tryck

EU

Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Europaparlamentets och rådets förordning 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

Fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt 2012/C 326/01

Kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag.

Sverige

Personuppgiftslag (1998:204)

Prop. 2017/18:105 Ny dataskyddslag

Litteratur

Bernitz, Ulf, Kjellgren, Anders. *Europarättens grunder. 5.* Uppl. Stockholm: Norstedts juridik, 2014.

Europeiska unionen. *Användarhandledning om definitionen av SMF-företag.* 2015. Hämtat från:
http://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0018.03/DOC_1

Korling, Fredrik, Zamboni, Mauro. *Juridisk metodlära*. 1. Uppl. Lund: Studentlitteratur, 2013.

Artiklar

Eriksson, William. Dagens Juridik. *Datainspektionen blir Integritetsskyddsmyndigheten - får 30 miljoner för satsning på GDPR*. Publicerad 2017-12-19. Senast hämtad 2018-05-18 från:
http://www.dagensjuridik.se/2017/12/datainspektionen-blir-integritetsskyddsmyndigheten-far-30-miljoner-satsning-pa-gdpr

Lindström, Andreas. Svenska Dagbladet. *Småföretagare hotas av miljonböter: ”Skrämmande”.* Publicerad 2018-04-09. Senast hämtad 2018-05-06 från:
https://www.svd.se/miljonboter-hotar-smaforetagare-skrammande

Mynewsdesk. *Två månader kvar: Bara fyra av tio småföretagare har satt sig in i GDPR.* Publicerad 2018-04-03. Senast hämtad 2018-05-06 från:

http://www.mynewsdesk.com/se/visma/pressreleases/tvaa-maanader-kvar-bara-fyra-av-tio-smaafoeretagare-har-satt-sig-in-i-GDPR-2456720
Mölne, Viktor. Dagens Industri. *Spelbolag stänger ner i Europa inför GDPR*. Publicerad 2018-05-16. Senast hämtad 2018-05-18 från:
https://www.di.se/nyheter/spelbolag-stanger-ner-i-europa-infor-gdpr/

Sveriges Radio. *Få fälls för misstänkta brott mot PUL*. Publicerad 2013-03-28. Senast hämtad 2018-05-06 från:
https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5487830

TT. Svenska Dagbladet. *GDPR kommer att kosta 2 000 miljarder kronor*. Senast hämtad 2018-05-22 från:
https://www.svd.se/gdpr-kommer-att-kosta-2000-miljarder-kronor

Internetkällor

Datainspektionen

Datainspektionen. *Ansvarsskyldighet*. Senast hämtad 2018-05-06 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/principer-for-behandling-av-personuppgifter/ansvarsskyldighet/

Datainspektionen. *Avtal med den registrerade*. Senast hämtad 2018-05-08 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/rattslig-grund-for-personuppgiftsbehandling/avtal/

Datainspektionen. *Dataskyddsförordningens grundläggande principer*. Senast hämtad 2018-06-17 från:
https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/

Datainspektionen. *Förberedelser för personuppgiftsansvariga*. Senast hämtad 2018-05-06 från:
https://www.datainspektionen.se/dataskyddsreformen/forberedelser/forberedelser-for-personuppgiftsansvariga/

Datainspektionen. *Hur vidtar vi lämpliga skyddsåtgärder?*. Senast hämtad 2018-06-16 från:
https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vidtar-vi-lampliga-skyddsatgarder/

Datainspektionen. *När ska vi informera de registrerade?*. Senast hämtad 2018-05-22 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/anmala-personuppgiftsincident/nar-ska-jag-informera-de-registrerade-/

Datainspektionen. *Personuppgifter i arbetslivet*. Senast hämtad 2018-05-22 från:
https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/arbetslivet/

Datainspektionen. *Personuppgifter och personuppgiftsbehandling*. Senast hämtad 2018-05-06 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/tillampningsomrade/personuppgifter-och-personuppgiftsbehandling/

Datainspektionen. *Principer för behandling av personuppgifter*. Senast hämtad 2018-05-06 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/principer-for-behandling-av-personuppgifter/

Datainspektionen. *Rättslig förpliktelse*. Senast hämtad 2018-05-08 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/rattslig-grund-for-personuppgiftsbehandling/rattslig-forpliktelse/

Datainspektionen. *Skydda grundläggande intressen*. Senast hämtad 2018-05-06 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/rattslig-grund-for-personuppgiftsbehandling/skydda-grundlaggande-intressen/

Datainspektionen. *Strukturerat eller ostrukturerat?*. Senast hämtad 2018-05-06 från:
https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/strukturerat-eller-ostrukturerat/

Datainspektionen. *Uppgift av allmänt intresse och myndighetsutövning*. Senast hämtad 2018-05-08 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/rattslig-grund-for-personuppgiftsbehandling/allmant-intresse/

Datainspektionen. *Uppgiftsminimering*. Senast hämtad2018-05-22 från:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/principer-for-behandling-av-personuppgifter/uppgiftsminimering/

Datainspektionen. *Vad menas med överföring till tredje land?*. Senast hämtad 2018-06-16 från:
https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverfo-ring/vad-menas-med-overforing-till-tredje-land/

Datainspektionen. *Överföring till tredje land*. Senast hämtad 2018-06-16 från:
https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/

Övrigt

Ekonomifakta. *Företagens storlek*. Senast hämtad 2018-05-06 från:
https://www.ekonomifakta.se/Fakta/Foretagande/Naringslivet/Naringslivets-struktur/

Verksamt. *GDPR-guiden*. Senast hämtad 2018-05-06 från:
https://www.verksamt.se/driva/GDPR-dataskyddsregler/GDPR-guiden

Bilaga – Svarsresultatet från min undersökning

Företag	Fråga 1	Fråga 2
Företag 1	Ja	Nej
Företag 2	Ja	Ja
Företag 3	Nej	
Företag 4	Ja	Ja
Företag 5	Ja	Ja
Företag 6	Ja	Nej
Företag 7	Ja	Nej
Företag 8	Nej	
Företag 9	Ja	Ja
Företag 10	Nej	
Företag 11	Nej	
Företag 12	Ja	Ja
Företag 13	Nej	
Företag 14	Ja	Nej
Företag 15		
Företag 16		
Företag 17	Nej	
Företag 18	Ja	Nej
Företag 19	Ja	Ja
Företag 20	Ja	Ja
Företag 21	Nej	
Företag 22	Ja	Ja
Företag 23	Ja	Nej
Företag 24		
Företag 25	Nej	
Företag 26	Ja	Ja
Företag 27	Nej	
Företag 28	Ja	Ja
Företag 29	Ja	Ja
Företag 30		