JURIDISKA INSTITUTIONEN
Stockholms universitet

Personuppgiftsbiträden enligt dataskyddsförordningen

- samma definition men en förändrad roll

Linda Olsson

Examensarbete i Rättsinformatik, 30 hp
Examinator: Mauro Zamboni
Stockholm, Höstterminen 2016

Stockholms universitet

Förord

Jag vill tacka min handledare Cecilia Magnusson Sjöberg för vägledning och feedback, Sara Edlund och Jens Kullander på Dustin AB samt medarbetare på Lindahl Advokatbyrå AB för värdefulla tips, råd och användbart material till denna uppsats. Jag vill även rikta ett stort tack till vänner och familj för det stöd och den omtanke ni gett mig under hela min utbildning. Tack.

Huddinge 2016-12-21
Linda Olsson

Abstract

On April 27 this year the European Parliament and the Council of the European Union published a new data protection law - "The General Data Protection Regulation" (GDPR). The new regulation aims to create a harmonized data protection legislation inside the European Union, to ensure an uniform protection of personal data and to avoid differences that may preclude the free movement of personal data within the internal market. The regulation is directly applicable and will therefore replace the national laws of data protection.

The new regulation contains a lot of news, for example heavy administrative fines and more obligations and responsibility for data processors. A data processor is a natural or legal person which processes personal data on behalf of a data controller. A data controller could be a company that process personal data about their costumers or employees. A data processor is for example a provider of IT-services, such as Microsoft. When the data controller enters personal data into a system that is provided by Microsoft, the service provider may store or in other way process the personal data on behalf of the controller. In such cases, Microsoft is a data processor.

The regulation means that the data processors will get more obligations and a new responsibility. This essay aims to analyze what these new obligations and this new responsibility means, and what consequences it could lead to. The new obligations include an obligation to inform the data controller about any new sub-processors, to inform the data controller about a data breach, to designate a data protection officer, and so on. The new responsibility means that the data processor can be directly charged by a data subject, which is not possible today. Also, the supervisor authority can impose administrative fines directly to the data processor. The consequences of these new rules could be, besides of some practical difficulties, that there no longer exists a clear line between the data controller and the data processor. The new rules could also have an economic effect on the data processors and their services and some special effects on cloud services. The General Data Protection Regulation will take an effect in May 25, 2018.

Begrepp

Personuppgifter:	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Med direkt identifikation menas att en person kan identifieras direkt genom en viss uppgift. Med indirekt identifikation menas att något behöver tillföras för att en identifikation ska kunna ske, t.ex. ytterligare en uppgift[1] eller en nyckel för att lösa en kryptering.[2] Exempel på personuppgifter är kontaktuppgifter, personnummer, kontouppgifter, IP-adresser, personliga preferenser, m.m.
Behandling av personuppgifter:	Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter. Som exempel kan nämnas insamling, lagring, användning, ändring, spridning, förstöring m.m.
Den registrerade:	Den som personuppgifterna avser. Med detta menas den person som kan identifieras med hjälp av personuppgifterna.
Personuppgiftsansvarig:	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Det företag som samlar in och behandlar uppgifter för sina kunder och anställda är ofta personuppgiftsansvarig.
Personuppgiftsbiträde:	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Företag:	Med företag avses i denna uppsats definitionen i 2 § 1 p. bokföringslag (1999:1078).
Tredje land:	Ett land utanför EU/EES.

[1] Europaparlamentet och Rådets Förordning (EU) av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46 EG

[2] Sjöberg, Personuppgiftslag (1998:204) 3 §, Lexino 2015-12-31

Innehållsförteckning

1. Inledning

1.1 Bakgrund

I takt med den digitala utvecklingen behandlas personuppgifter i allt större omfattning. När en kund köper en produkt via internet ställer företagen ofta som krav att kunden ska registrera sitt namn, telefonnummer, sin leveransadress samt mailadress för att köpet ska kunna fullföljas. Det är även vanligt att företag placerar ut cookies på en kunds dator när kunden besöker företagets hemsida. En cookie är en textfil som placeras på kundens hårddisk och som ger företaget information om bland annat vilka produkter kunden verkar vara intresserad av. På så sätt kan företaget styra framtida reklam, nyhetspresentationer m.m.[3] Detta är endast två av väldigt många exempel på när ett företag insamlar personuppgifter från kunder. Utöver kunduppgifter behandlar även företag personuppgifter från anställda och leverantörer. Sammantaget behandlar ett företag väldigt många personuppgifter.

Ett företag får dock inte behandla personuppgifter hur som helst. Skyddet av personuppgifter är en mänsklig rättighet[4] och enligt 1 § personuppgiftslagen (1998:204) kan en felaktig behandling innebära en kränkning av en människas personliga integritet. Det finns därför regelverk som bestämmer hur personuppgifter får behandlas. För svensk del består regelverket idag av dataskyddsdirektivet[5] som implementerats i svensk rätt genom den ovan nämnda personuppgiftslagen. Det finns även en mängd registerförfattningar som kompletterar personuppgiftslagen, framför allt vad gäller myndigheters personuppgiftsbehandling.[6]

När dataskyddsdirektivet tillkom var syftet att åstadkomma ett starkt och harmoniserat skydd för personuppgifter i medlemsstaterna.[7] Unionens medlemsstater implementerade dock dataskyddsdirektivet på olika sätt, vilket resulterat i en bristfällig enhetlighet.[8] Enligt EU är en harmoniserad integritetslagstiftning en garanti för den inre digitala marknaden.[9] Eftersom personuppgifter behandlas i allt större omfattning och det råder en bristande enhetlighet i unionen vad gäller skyddet av dessa uppgifter, anser EU att det behövs tydligare reglering på

[3] Magnusson Sjöberg, Cecilia (red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2 u., Studentlitteratur AB, Lund, 2016, s. 349
[4] Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02), artikel 8
[5] 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 (Dataskyddsdirektivet)
[6] Magnusson Sjöberg, Cecilia (red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2 u., Studentlitteratur AB, Lund, 2016, s. 212
[7] Dataskyddsdirektivet, skäl 7
[8] Dataskyddsförordningen, skäl 9
[9] Dataskyddsdirektivet, skäl 7

området. Resultatet av detta publicerades den 27 april i år, nämligen EU:s allmänna dataskyddsförordning.[10]

Förordningen kommer ersätta dataskyddsdirektivet och personuppgiftslagen och blir direkt tillämplig i medlemsstaterna den 25 maj 2018. Dataskyddsförordningen ger de registrerade fler rättigheter än dataskyddsdirektivet, vilket ställer högre krav på företags och andra juridiska personers rutiner kring personuppgiftshantering. Dessutom inträder betungande sanktioner för den som bryter mot förordningens regler. Konsekvensen av detta blir att företag och andra juridiska personer nu måste lägga ner mycket arbete på att förändra verksamhetens personuppgiftsbehandling för att uppfylla förordningens krav.

Under tiden som jag författat detta examensarbete har jag deltagit i ett sådant förändringsarbete. Jag har nämligen gjort min uppsatspraktik på Dustin AB, ett företag som är återförsäljare av IT-produkter med tillhörande tjänster. På Dustin har jag varit en del av företagets DPP (Data Protection Project) och därmed fått ta del av den förändring som dataskyddsförordningen innebär för ett företag i praktiken. Dustins förändringsarbete började exempelvis med en kartläggning. Under denna kartläggning utredde Dustin vilka personuppgifter som företaget behandlar samt hur och var behandlingen sker. I skrivande stund är kartläggningen klar och nästa fas har precis börjat – nämligen att analysera kartläggningen och upptäcka eventuella brister. Steget efter detta blir att hitta nya rutiner och säkerhetsåtgärder för att åtgärda eventuella brister innan förordningens ikraftträdande. Under projektets gång har det bland annat uppkommit frågor kring Dustins ansvar som personuppgiftsbiträde.

Ett personuppgiftsbiträde är, enligt 3 § personuppgiftslagen, någon som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Personuppgiftsansvarig är enligt samma lagrum den som, ensam eller tillsammans med andra, bestämmer ändamålet med och medlen för behandlingen av personuppgifter. Sett ur ett företagsperspektiv är en personuppgiftsansvarig normalt det företag som i sin verksamhet samlar in och behandlar personuppgifter om sina anställda eller kunder. Det är själva företaget som juridisk person som är personuppgiftsansvarig och inte exempelvis chefen på arbetsplatsen.[11] Ett personuppgiftsbiträde är alltså någon som behandlar personuppgifter för det nämnda företagets räkning. Exempelvis är Dustin ett personuppgiftsbiträde eftersom Dustin erbjuder IT-tjänster av olika slag, bland annat är företaget återförsäljare av flera av Microsofts molntjänster. Om kunden

[10] Europaparlamentet och Rådets Förordning (EU) av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46 EG

[11] Christner, Anders och Edvardsson, Tobias, *Cloud Computing – en handledning och kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010*, 2011, s. 43

köper tjänsten via Dustin sköter Dustin bland annat underhåll, övervakning, administration och support åt kunden. Detta innebär att Dustin kommer att behandla personuppgifter åt kundens räkning och Dustin blir därmed ett personuppgiftsbiträde.

Att det uppkommit frågor i projektet angående Dustins roll som personuppgiftsbiträde beror på att dataskyddsförordningen kommer att innebära stora förändringar för personuppgiftsbiträden. Personuppgiftsbiträdet kommer att få fler skyldigheter, ett större ansvar och dessutom blir sanktionerna kraftigare. När förordningen träder ikraft kommer Datainspektionen ha befogenhet att utfärda administrativa sanktionsavgifter gentemot den som bryter mot förordningens regler. En sådan avgift kan uppgå till 20 000 EUR eller 4 % av den totala globala årsomsättningen. Eftersom sanktionerna är betungande är det av intresse att undersöka vad personuppgiftsbiträdet måste göra för att uppfylla förordningens krav. Uppsatsen ska därför belysa vilka nya skyldigheter och vilket ansvar som biträdena kommer påföras samt analysera vilka kortsiktiga och långsiktiga problem som kan uppkomma på grund av de nya reglerna.

1.2 Syfte och frågeställning

Syftet med uppsatsen är att undersöka och analysera hur personuppgiftsbiträdets skyldigheter och ansvar kommer att förändras när förordningen börjar gälla, samt vilka konsekvenser som kan uppkomma. De frågor som ska besvaras är således;

- Hur förändras personuppgiftsbiträdets skyldigheter och vilka praktiska frågor och problem kan skyldigheterna ge upphov till?
- Hur kommer ansvarsfördelningen mellan personuppgiftsansvarig och personuppgiftsbiträde att förändras och kommer det kunna påverkas genom avtal?
- Vilka konsekvenser kan de nya reglerna komma att få för personuppgiftsbiträden?

1.3 Avgränsning

Uppsatsen är skriven utifrån ett företagsperspektiv, det vill säga vilka skyldigheter och vilket ansvar ett företag, som är leverantör av en IT-tjänst, kommer få när förordningen träder ikraft. Anledningen till detta är att jag under skrivandets gång praktiserat på ett företag och därför uppmärksammat frågor och problem som förordningen kan innebära för ett företag. Uppsatsen behandlar därför inte andra juridiska personer, som myndigheters och kommuners, behandling av personuppgifter. Detta utesluter inte att även dessa personuppgiftsbiträden kan använda denna uppsats som en vägledning.

1.4 Metod och material

För att påvisa de förändringar som kommer ske för personuppgiftsbiträden jämför uppsatsen genomgående de regler som gäller i Sverige idag med de regler som kommer gälla när dataskyddsförordningen träder ikraft. För att kunna göra denna jämförelse fastställs för det första vilken som är den gällande rätten idag, exempelvis vilka skyldigheter och vilket ansvar som personuppgiftsbiträden har i dataskyddsdirektivet och personuppgiftslagen. För att fastställa denna rätt tillämpas och tolkas traditionella rättskällor som lag, förarbeten och doktrin - det används således en rättsdogmatisk metod.[12] Jag har även använt mig av mindre traditionella rättskällor som lagkommentarer och information från Datainspektionen. Lagkommentarer har jag använt mig av för att själv få en ökad förståelse och hitta viktiga hänvisningar till rättskällor. Eftersom Datainspektionen är en så pass viktig myndighet i sammanhanget har jag även använt deras information som ett verktyg för förståelse.

Utöver svenska rättskällor används till stor del även EU:s rättsakter, exempelvis dataskyddsdirektivet samt dataskyddsförordningen. Den rättsdogmatiska metoden kombineras således även med en EU-rättslig metod. Vid tolkningen av de EU-rättsliga akterna har jag tagit vägledning från de skäl som anges i början av direktivet och förordningen. Jag har även tagit stöd av Europeiska Kommissionens, Europaparlamentets samt artikel 29-arbetsgruppens yttranden för tolkning av materialet. Artikel 29-arbetsgruppen har fått sitt namn från artikel 29 i dataskyddsdirektivet, och har till uppgift att vara rådgivande, oberoende och bidra till en enhetlig tillämpning av direktivets bestämmelser. De olika yttranden som nyss nämnts är inte bindande, utan dessa yttranden tillhör det som i EU-rätten kallas ”soft law”. Soft law kan i praktiken bli bindande, om annat tolkningsmaterial saknas.[13] EU-domstolen har till och med uttryckt att nationella myndigheter och domstolar kan ha en skyldighet att följa soft law.[14]

Uppsatsen har även inslag av rättsinformatisk metod. Metoden innebär att rättsfrågor som har med utveckling, införande, användning och förvaltning av olika IT-system aktualiseras.[15] Eftersom denna uppsats analyserar svårigheter och problem som kan uppstå när dataskyddsförordningen ska tillämpas vid användningen av IT-system, används också en rättsinformatisk metod i uppsatsen.

---

[12] Korling, Fredric och Zamboni, Mauro (Red.) *Juridisk metodlära*, 1.5 u., Studentlitteratur AB, Lund, 2015, s. 21

[13] Korling, Fredric och Zamboni, Mauro (Red.) *Juridisk metodlära*, 1.5 u., Studentlitteratur AB, Lund, 2015, s. 127 f.

[14] Mål C-322/88, Grimaldi mot Fonds des maladies professionnelles, ECLI:EU:C:1989:646

[15] Magnusson Sjöberg, Cecilia (Red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2:a u., Studentlitteratur AB, Lund, 2016, s. 27

1.5 Disposition

Dispositionen av denna uppsats har till syfte att göra framställningen så pedagogisk som möjligt. Därför besvarar uppsatsen frågor i en viss ordning som ger framställningen en logisk röd tråd. Innan varje kapitel finns även ett inledande avsnitt som förklarar varför kapitlet är viktigt för frågeställningen. Den första frågan som uppsatsen besvarar är vem som är ett personuppgiftsbiträde. Denna fråga är grundläggande för den senare framställningen, eftersom den avgör vem som omfattas av de nya reglerna. När det är utrett vem som är ett personuppgiftsbiträde besvarar uppsatsen nästa fråga, nämligen vilka skyldigheter ett sådant biträde har och hur dessa skyldigheter kommer förändras. Den tredje frågan handlar om vilka sanktioner som kan inträda om skyldigheterna i förordningen inte uppfylls. Därefter undersöker uppsatsen när ett personuppgiftsbiträde kan bli ansvarigt för en sådan sanktion, det vill säga hur ansvarsfördelningen mellan personuppgiftsansvarig och biträden kommer att se ut. Uppsatsen har en löpande analys genom hela framställningen. Vissa större frågor om reglernas konsekvenser för personuppgiftsbiträden har dock ett eget kapitel i slutet av uppsatsen.

2. Begreppet personuppgiftsbiträde

2.1 Inledning

I detta kapitel ska begreppet personuppgiftsbiträde förklaras mer ingående än den kortfattade beskrivning som gavs under avsnittet ”Begrepp” ovan. Att klargöra vem som är ett personuppgiftsbiträde är centralt för framställningen eftersom det avgör vem som omfattas av de nya regler som kommer behandlas i denna uppsats. Legaldefinitionen av ett personuppgiftsbiträde är enligt 3 § personuppgiftslagen ”Den som behandlar personuppgifter för den personuppgiftsansvariges räkning”. En aktuell fråga är vad denna definition innebär i praktiken? För att besvara frågan kan sägas att ett personuppgiftsbiträde som huvudregel är leverantör av en tjänst till den personuppgiftsansvarige. Tjänsten kan t.ex. bestå i att tillhandahålla ett system, en server[16] eller olika supporttjänster. När ett företag tillhandahåller en sådan tjänst kan företaget komma att behandla de uppgifter som den personuppgiftsansvarige t.ex. matat in i systemet. På så sätt behandlar leverantören av tjänsten uppgifter för den personuppgiftsansvariges räkning och leverantören blir ett personuppgiftsbiträde, medan kunden som köper tjänsten är personuppgiftsansvarig.

Detta kapitel har till syfte att ge exempel på leverantörer som omfattas av begreppet personuppgiftsbiträde, för att öka förståelsen för begreppet och ge detta en verklighetsförankring. Kapitlet uppmärksammar sedan vem som inte ska blandas ihop med ett personuppgiftsbiträde och i samband med detta analyserar framställningen vissa avgränsningsproblem.

2.2 Molntjänstleverantörer

Ett första exempel på en leverantör som omfattas av begreppet personuppgiftsbiträde är molntjänstleverantören. Molntjänst är en IT-tjänst som blir allt vanligare på marknaden. Begreppet har ingen generellt accepterad definition och är inte helt lätt att beskriva på grund av dess varierande karaktär. Det finns dock en definition som det refereras till i rättskällor[17] och som framtagits av NIST (US National Institute for Standards and Technology).[18] Denna definition kan användas som vägledning i frågan vad som utgör en molntjänst och fungerar oavsett om

[16] En server är en dator som förser ett datanät med gemensamma servicefunktioner, t.ex. datalagring och e-postkommunikation. (källa: Nationalencyklopedin, server. http://www.ne.se.ezp.sub.su.se (hämtad 2016-12-13))
[17] Se t.ex. Magnusson Sjöberg, Cecilia (Red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2:a u., Studentlitteratur AB, Lund, 2016, s. 442 och SOU 2016:41 s. 562
[18] National Institute of Standards and Technology Special Publication 800-145, The NIST Definition of Cloud Computing, september 2011

man söker svaret utifrån ett tekniskt, affärsmässigt eller legalt perspektiv.[19] Definitionen är följande;

”Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Till sin definition tillägger NIST att en molntjänst består av fem olika karaktärsdrag, tre tjänstemodeller och fyra leveransmodeller.[20] Det första karaktärsdraget är att en molntjänst ska ha en ”on-demand self service”. Med detta menas att kunden inte behöver ta kontakt med leverantören för att kunna använda tjänsten, utan det är kunden självständigt som ska kunna välja, starta och avsluta molnleverantörens tjänst. Exempelvis kan nämnas när en person skapar ett gmail-konto. Kontot kan skapas utan någon kontakt med leverantören och uppfyller således kravet på ”on-demand self service”. Det andra karaktärsdraget benämner NIST ”Broad network access”. Med detta menas att tjänsten ska vara tillgänglig över hela världen om kunden har tillgång till en enhet, t.ex. dator, surfplatta eller mobil, som kan uppkopplas till internet.

Ett tredje och väsentligt karaktärsdrag kallas ”Resource pooling”. Med detta menas att en tjänst, för att utgöra en molntjänst, ska uppfattas som ett system av kunden. Kunden ska inte behöva veta var leverantörens servrar är placerade, hur tjänsten är uppbyggd tekniskt m.m. Det fjärde karaktärsdraget kallas ”Rapid elasticity”. Detta karaktärsdrag innebär att kunden inte behöver bestämma kapacitetsramarna i förväg. Kapaciteten anpassar sig efter användandet. Det femte och sista karaktärsdraget benämns ”Measured service”. Med detta menas att kunden endast betalar för så mycket av tjänsten som kunden nyttjar.

Om en tjänst uppfyller alla de fem karaktärsdragen är det fråga om en molntjänst. Enligt NIST kan molntjänster vidare delas upp i 3 olika tjänstemodeller. Vilken modell som kunden väljer beror på hur mycket kontroll över tjänsten kunden vill ha själv och hur mycket kontroll som överlåts till leverantören. Den första tjänstemodellen kallas ”Software as a Service” (SaaS). Vid användandet av denna modell har kunden knappt någon egen kontroll alls utan är

[19] Magnusson Sjöberg, Cecilia (Red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2:a u., Studentlitteratur AB, Lund, 2016, s. 442

[20] Angående den följande framställningen, se Magnusson Sjöberg, Cecilia (Red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2:a u., Studentlitteratur AB, Lund, 2016, s. 443-447 samt National Institute of Standards and Technology Special Publication 800-145

endast en användare av ett system som tillhandahålls över internet. Som exempel på SaaS-tjänster kan nämnas Gmail eller Facebook. Den andra modellen kallas ”Platform as a Service” (PaaS) och ger kunden mer kontroll över tjänsten än vad en SaaS-tjänst gör. Tjänsten ger kunden tillgång till en stabil plattform med färdiga funktioner för att kunden ska kunna utveckla egna datorprogram som körs som molntjänster. Exempel på PaaS-tjänster är Google Apps och Microsoft Azure. Den sista tjänstemodellen är den modell som ger kunden mest kontroll, och kallas ”Infrastructure as a Service” (IaaS). Denna tjänst ger kunden direkt kontroll över grundläggande infrastrukturresurser som lagring, nätverk och beräknings-kapacitet. Observera att kunden inte får tillgång till leverantörens direkta hårdvara, eftersom då det tredje karaktärsdraget för en molntjänst (Resource pooling) hade gått förlorat.

Slutligen kan en molntjänst enligt NIST delas upp i fyra olika leveransmodeller. Den första modellen kallas ”Private cloud”. Tjänsten levereras då till en enskild organisation som är den enda som har tillgång till tjänsten. Den andra leveransmodellen kallas ”Community cloud”. Denna leveransmodell innebär att det är flera specifika organisationer som har tillgång till tjänsten, t.ex. flera företag i en koncern.[21] Den tredje leveransmodellen kallas ”Public Cloud” och är till för alla som vill nyttja den, t.ex. Google mail eller Dropbox. Den fjärde och sista leveransmodellen kallas ”Hybrid cloud” och är en kombination av ovanstående modeller.

Som framställningen ovan visat finns det många olika typer av molntjänster. Ett företag som köper en molntjänst är ofta personuppgiftsansvarig, medan leverantören blir ett personuppgiftsbiträde. Molntjänstleverantören behandlar personuppgifter åt den personuppgifts-ansvarige vid t.ex. lagring av uppgifter i molnet.

2.3 Andra personuppgiftsbiträden

Det finns personuppgiftsbiträden som levererar andra tjänster än molntjänster. Bland annat finns det en tjänst som kallas ”server hosting”. Kunden äger då en egen server där alla person-uppgifter lagras, men servern befinner sig hos en leverantör som sköter drift av servern. Kunden har inte tillgång till servern, utan det har endast leverantören. Det är således leverantören som ska se till att servern fungerar som den ska och åtgärda eventuella problem som uppkommer.

En annan tjänst kallas ”CO-location” och påminner om ”server hosting”, skillnaden ligger i att kunden har tillgång till servern och endast hyr plats i leverantörens driftshall. En sådan driftshall är uppbyggd för ändamålet att förvara servrar och kan därför erbjuda hög

[21] En speciell form av community cloud är myndighetsmoln (government cloud) som används t.ex. i Storbritannien. Myndighetsmolnet är ett moln som ska möta särskilda behov av t.ex. säkerhet.

säkerhet och bra anslutning till nätverk. Vidare finns det en tjänst som kallas ”dedikerad servertjänst”. Detta innebär att leverantören äger servern och kunden hyr utrymme på denna server, som är placerad hos leverantören. Det finns även en tjänst som beskrivs som ”fullständig outsourcing”. Med fullständig outsourcing menas att all IT-verksamhet överlåts till en extern leverantör. [22] Även om servern är lokaliserad hos den personuppgiftsansvarige kan det finnas ett personuppgiftsbiträde. Företag som anlitas för underhåll av servern, t.ex. avhjälpande av ett fel, uppdateringar eller andra supporttjänster, är också personuppgiftsbiträden.[23]

Vad gäller ”server hosting”, ”dedikerad servertjänst” och ”fullständig outsourcing” är leverantören ett personuppgiftsbiträde eftersom leverantören kommer att behandla personuppgifterna vid drift av servern. Vad gäller de två sista alternativen äger till och med leverantören servern och lagrar därför personuppgifter för den personuppgiftsansvariges räkning.

Vad gäller ”Co-location” bör det dock kunna ifrågasättas om leverantören verkligen behandlar personuppgifter för den personuppgiftsansvariges räkning. Att endast förvara någon annans server bör inte kunna räknas som att behandla personuppgifter. Det bör kunna likställas med att förvara ett USB-minne innehållande personuppgifter i ett bankfack. Innebär detta att banken är ett personuppgiftsbiträde? Antagligen inte. Om en leverantör av tjänsten ”Co-location” ska räknas som ett personuppgiftsbiträde bör leverantören sköta driften av servern eller på annat sätt behandla personuppgifterna som finns på servern.

2.4 Underbiträden

Ett personuppgiftsbiträde kan anlita underbiträden, eller underleverantörer som de ofta kallas. Skäl för att anlita ett underbiträde kan vara kostnader, kompetens eller tidsramar.[24] Det är särskilt vanligt med underbiträden när det kommer till molntjänster. Dataskyddsdirektivet, personuppgiftslagen eller dataskyddsförordningen gör ingen skillnad mellan ett personuppgiftsbiträde och ett underbiträde. Således gäller samma regler för alla biträden. Regelverken ställer krav på att den personuppgiftsansvarige har ett personuppgiftsbiträdesavtal med varje biträde, således även underbiträden. I praktiken brukar detta lösas genom att den personuppgiftsansvariga i avtalet med en leverantör ger detta personuppgiftsbiträde en fullmakt att ingå

[22] Perméus, Anders och Lindberg, Daniel, *IT-avtal – En kommentar till IT-branschens standardavtal*, Jure Förlag AB, Stockholm, 2013, s. 328
[23] Perméus, Anders och Lindberg, Daniel, *IT-avtal – En kommentar till IT-branschens standardavtal*, Jure Förlag AB, Stockholm, 2013, s. 437
[24] Sjöberg, Personuppgiftslag (1998:204) 30 §, Lexino 2015-12-31

avtal med eventuella underleverantörer.[25] Vilken informationsskyldighet som personuppgiftsbiträdet har gentemot den personuppgiftsansvarige angående eventuella underbiträden framgår av kapitel 3.2.2.

2.5 Avgränsning av begreppet personuppgiftsbiträde

2.5.1 Personuppgiftsansvarig

Det finns begrepp i dataskyddsförordningen som ska avgränsas från begreppet personuppgiftsbiträde. Det första begreppet som inte ska sammanblandas med ett personuppgiftsbiträde är den personuppgiftsansvarige. Detta kanske ses som en självklarhet men i praktiken kan det finnas vissa gränsdragningsproblem. Som beskrivits ovan i det inledande kapitlet är en personuppgiftsansvarig den som bestämmer ändamålen med och medlen för behandlingen. Med ändamål och medel menas i princip *varför* och *hur* personuppgifterna behandlas.[26] Ibland kan det dock vara oklart vem det är som faktiskt bestämmer.

Ett exempel på detta är fallet SWIFT som artikel 29-arbetsgruppen har analyserat.[27] Företaget SWIFT (Society for Worlwide Interbank Financial Telecommunication) tillhandahöll en tjänst (SWIFTNet FIN) som gick ut på att överföra bankuppgifter från europeiska finansinstitut till amerikanska myndigheter, i syfte att förhindra terrorism. SWIFT ansåg sig endast som en förmedlare av uppgifterna och därmed endast som ett personuppgiftsbiträde. I avtalen mellan SWIFT och finansinstituten benämndes SWIFT som ”underleverantör”.[28] Med beaktande av att SWIFT:s styrelse bestämde både ändamålen med och medlen för behandlingen av personuppgifter och genomförde förhandlingar med amerikanska myndigheter utan finansinstitutens insyn, sågs SWIFT som personuppgiftsansvarig istället för ett personuppgiftsbiträde/underbiträde.[29]

Det gränsdragningsproblem som beskrivs i SWIFT-fallet är vanligt när det kommer till molntjänster. Traditionellt sett är kunden personuppgiftsansvarig och molntjänstleverantören ett personuppgiftsbiträde. Om kunden är ett litet företag jämfört med leverantören kan det dock finnas risk för ombytta roller, eftersom det kan vara svårt för kunden att påverka och

[25] Christner, Anders och Edvardsson, Tobias, *Cloud Computing – en handledning och kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010*, 2011, s. 44
[26] Artikel 29-arbetsgruppens yttrande 1/2010 om begreppen registeransvarig och registerförare, antaget den 16 februari 2010, s. 13.
[27] Artikel 29-arbetsgruppens yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society för Worldwide Interbank Financial Telecommunication) antaget den 22 november 2006
[28] Artikel 29-gruppens yttrande 10/2006 om behandling av personuppgifter hos SWIFT, s. 11
[29] Artikel 29-gruppens yttrande 10/2006 om behandling av personuppgifter hos SWIFT, s. 12

kontrollera hur leverantören behandlar personuppgifterna i molnet.[30] Eftersom medlen för behandlingen ofta är en teknisk fråga kan denna bestämmanderätt till viss del delegeras till biträdet utan att rollerna skiftar. För att detta ska fungera krävs dock att den personuppgiftsansvariga får fullständig information om vilka medel som leverantören kommer använda samt att viktiga frågor som avgör om behandlingen är tillåten fortfarande avgörs av den personuppgiftsansvariga.[31] Om det framgår att det är personuppgiftsbiträdet som egentligen bestämmer ändamålet med och medlen för behandlingen ska personuppgiftsbiträdet ses som en personuppgiftsansvarig vad avser den behandlingen. Denna regel har tagits in i dataskyddsförordningen artikel 28.10.

2.5.2 Tredje part

Ett annat begrepp som ska avskiljas från personuppgiftsbiträde är begreppet *tredje man,* eller som dataskyddsförordningen benämner begreppet; *tredje part*. Likheten mellan ett personuppgiftsbiträde och en tredje part är att de båda får tillgång till den personuppgiftsansvarigas personuppgifter. Skillnaden ligger i att personuppgiftsbiträdet är bunden av den personuppgiftsansvarigas instruktioner, medan tredje part inte är det. Ett vanligt exempel på en sådan tredje part är myndigheter, t.ex. Skatteverket. Ett företag är skyldigt att överföra personuppgifter om sina anställda till Skatteverket, t.ex. vid inlämnandet av kontrolluppgifter. Att Skatteverket tar emot och behandlar dessa personuppgifter innebär inte att Skatteverket är ett personuppgiftsbiträde. Skatteverket är nämligen inte bunden av den personuppgiftsansvariges instruktioner, myndigheten får behandla personuppgifterna utan den personuppgiftsansvariges insyn.

En myndighet är dock inte alltid en tredje part utan kan även vara ett personuppgiftsbiträde. I dessa fall är myndigheten ofta ett personuppgiftsbiträde åt en annan myndighet genom att IT-drift levereras från en myndighet till en annan. Det förekommer även att myndigheter är personuppgiftsbiträden åt enskilda.[32] Av denna anledning kan det ibland vara svårt att dra en skarp gräns angående vem som är ett personuppgiftsbiträde och vem som är tredje part. För att kunna avgöra detta behöver undersökas om myndigheten är bunden av den personuppgiftsansvariges instruktioner eller inte.

Som ett exempel på ett annat gränsdragningsproblem mellan begreppen personuppgiftsbiträde och tredje part kan nämnas ett företag som handhar uppgifter om anställdas pension för den personuppgiftsansvariga. Är detta företag ett personuppgiftsbiträde eller en tredje

[30] Sjöberg, Personuppgiftslag (1998:204) 3 §, Lexino 2015-12-31
[31] Artikel 29-arbetsgruppens yttrande 1/2010 om begreppen registeransvarig och registerförare, antaget den 16 februari 2010, s. 14 f.
[32] SOU 2015:39, s. 337

part? På samma sätt som ovan beror svaret på om företaget behandlar uppgifterna efter den personuppgiftsansvarigas instruktioner eller inte. Om företaget måste återföra eller förstöra alla personuppgifter när den anställda slutar arbeta hos den personuppgiftsansvarige, är företaget antagligen ett personuppgiftsbiträde. Om företaget däremot får fortsätta att behandla uppgifter för den anställda även när denna byter arbetsplats, är företaget antagligen en tredje part. För att avgöra om ett företag är ett personuppgiftsbiträde eller tredje part måste således tas hänsyn till företagets beroendeställning gentemot den personuppgiftsansvarige.

2.5.3 Mottagare och medhjälpare

I Dataskyddsförordningen återfinns även begreppet mottagare. En mottagare kan vara både en fysisk eller en juridisk person. Som mottagare räknas alla som tillförs personuppgifter, exempelvis personuppgiftsansvarig, personuppgiftsbiträde, tredje part och även den registrerade själv.[33] Bara för att någon är mottagare av personuppgifter är det alltså inte självklart att mottagaren omfattas av de regler som gäller för personuppgiftsbiträden, vilket förklarades i genomgången ovan om tredje part.

Medhjälpare är ett annat begrepp som ska avskiljas från personuppgiftsbiträde. Skillnaden mellan begreppen kan förklaras med att en medhjälpare behandlar personuppgifter *under* den personuppgiftsansvariga, medan ett personuppgiftsbiträde behandlar personuppgifter *för* den personuppgiftsansvariga. Ett exempel på en medhjälpare kan vara en arbetstagare som arbetar hos den personuppgiftsansvariga. En medhjälpare är vanligtvis en fysisk person. Det har dock varit uppe till diskussion om även en juridisk person skulle kunna vara en medhjälpare.[34] Om en medhjälpare kan vara en juridisk person finns det ett avgränsningsproblem även här. Hur avgör man om ett företag arbetar under eller för den personuppgiftsansvariga? Eftersom en medhjälpare inte omfattas av de regler som gäller för personuppgiftsbiträden, är det viktigt att kunna skilja de två begreppen åt. Det kan dock bli svårt med en sådan gränsdragning eftersom både medhjälparen och personuppgiftsbiträdet lyder instruktioner från den personuppgiftsansvariga. Möjligen är detta anledningen till att Datalagskommittén uttalade i ett av sina betänkanden att bara fysiska personer kan betraktas som medhjälpare.[35]

[33] Undantag för juridiska personer när de utför vissa myndighetsutövningar, Sjöberg, Personuppgiftslag (1998:204) 3 §, Lexino 2015-12-31
[34] Sjöberg, Personuppgiftslag (1998:204) 3 §, Lexino 2015-12-31
[35] Sjöberg, Personuppgiftslag (1998:204) 3 §, Lexino 2015-12-31, med hänvisning till SOU 1997/39 s. 336 f.

3. Personuppgiftbiträdets skyldigheter

3.1 Inledning

I föregående kapitel har framställningen redogjort för vem som är ett personuppgiftsbiträde. När ett företag omfattas av detta begrepp uppkommer vissa skyldigheter för företaget vad gäller behandlingen av personuppgifter. När förordningen träder i kraft kommer personuppgiftsbiträdets skyldigheter att bli mer omfattande. Detta kapitel har till syfte att beskriva hur personuppgiftsbiträdets nuvarande skyldigheter kommer förändras samt vilka helt nya skyldigheter som kommer tillkomma. I slutet av varje avsnitt uppmärksammar framställningen, när det behövs, vilka praktiska problem som de förändrade och nya skyldigheterna kan medföra.

3.2 Dataskyddsförordningens förändring av nuvarande skyldigheter

3.2.1 Ingå personuppgiftsbiträdesavtal

Enligt dataskyddsdirektivet artikel 17.3 och 30 § 2 stycket personuppgiftslagen ska den personuppgiftsansvarige och personuppgiftsbiträdet ingå ett personuppgiftsbiträdesavtal med varandra. Enligt regelverken ska detta avtal dels reglera att biträdet endast får behandla personuppgifter efter den personuppgiftsansvariges instruktioner, dels att biträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna. Eftersom regleringen inte gör någon åtskillnad mellan personuppgiftsbiträden och underbiträden måste den personuppgiftsansvarige även ingå avtal med underbiträden. Ett personuppgiftsbiträdesavtal ska vara skriftligt, antingen i pappersformat eller elektroniskt format. Det finns dock inget underskriftskrav.[36]

Skyldigheten att ingå ett personuppgiftsbiträdesavtal kommer finnas kvar när förordningen träder ikraft, vilket framgår av dataskyddsförordningen artikel 28.3. Formkravet för avtalet kommer enligt artikel 28.9 fortfarande vara skriftlighet, inbegripet elektroniskt format. Dataskyddsförordningen innebär dock en del förändringar. En förändring är att avtalsinnehållet kommer bli mycket mer detaljreglerat än tidigare.

I dataskyddsförordningen artikel 28.3 ställs fler krav på innehållet, bland annat ska avtalen ange ändamålen med behandlingen, behandlingens varaktighet, typ av personupp-

[36] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 434

gifter, kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter. Dataskyddsförordningen räknar sedan upp ett flertal olika skyldigheter för personuppgiftsbiträdet som särskilt ska regleras i avtalet. Dessa skyldigheter kommer beskrivas nedan.

Den förändring som förordningen kräver av personuppgiftbiträdesavtalen medför ett praktiskt problem, nämligen hur företagen ska agera när ett nytt personuppgiftsbiträde ska anlitas under den period som gäller fram till den 25 maj 2018. När ett personuppgiftbiträdesavtal ingås mellan två företag granskar ofta företagens jurister avtalet och kommer med vissa synpunkter innan företagen kommer överens. Det mest ekonomiska och effektiva för företagen när ett nytt biträde ska anlitas vore därför att de nya avtal som ingås uppfyller de krav som förordningen ställer. På så sätt behöver företagen inte ta sig tid att granska avtalen två gånger. Det finns dock ett problem. Det är inte säkert, och i skrivande stund inte särskilt troligt, att biträdet ännu har kommit så långt i förändringsprocessen att biträdet kan uppfylla alla de skyldigheter som det nya avtalet kommer kräva. Så fort biträdet skriver på avtalet finns det således en risk att biträdet kommer begå avtalsbrott. En lösning på problemet skulle kunna vara att ha ett avtal som gäller fram till den 25 maj 2018 och ett avtal som är klart och redo att börja gälla efter den 25 maj 2018.

3.2.2 Informationsskyldighet angående anlitande av underbiträden

En annan skyldighet som förändras handlar om personuppgiftsbiträdets informationskrav gentemot den personuppgiftsansvariga vad gäller anlitandet av underbiträden. Som nämnts i kapitel 2.4 kan ett personuppgiftsbiträde anlita ett underbiträde. Eftersom även ett underbiträde räknas som ett personuppgiftsbiträde enligt dataskyddsdirektivet och personuppgiftslagen ska den personuppgiftsansvariga ingå ett biträdesavtal med underbiträdet. Denna skyldighet delegeras som sagt ofta till personuppgiftsbiträdet.

Enligt dataskyddsdirektivet artikel 10 c) måste den personuppgiftsansvarige informera den registrerade om vilka som är mottagare till personuppgifterna, i den utsträckning som uppgifterna är nödvändiga för att den registrerade ska få en korrekt behandling. Denna bestämmelse har implementerats i 25–26 §§ personuppgiftslagen, där det anges att den registrerade ska få information från den personuppgiftsansvarige angående vilka som är mottagare till personuppgifterna. Vid en bedömning enligt personuppgiftslagens regler räcker det om den personuppgiftsansvarige lämnar information angående till vilka olika kategorier av

mottagare som uppgifterna lämnas till.[37] Observera att detta enligt regelverken är en skyldighet för personuppgiftsansvariga och inte för personuppgiftsbiträden.

Enligt artikel 29-arbetsgruppen innebär dock dataskyddsdirektivets artikel 10 c) även att personuppgiftsbiträden måste lämna information om underbiträden till den personuppgiftsansvarige. Enligt arbetsgruppen har personuppgiftsbiträdet en tydlig skyldighet att meddela den personuppgiftsansvarige om eventuella planerade förändringar, t.ex. om ett underbiträde läggs till eller tas bort. Arbetsgruppen anser även att personuppgiftsbiträdet bör ha en tydlig skyldighet att ange alla underbiträden som anlitas.[38] Som nämnts i metodavsnittet är artikel 29-arbetsgruppens yttranden formellt sett inte bindande, men kan i praktiken få den karaktären om annat tolkningsmaterial saknas.[39]

Av framställningen i detta avsnitt framgår att det idag finns en skyldighet för den personuppgiftsansvarige att veta vem som behandlar personuppgifterna och var behandlingen sker, vilket enligt artikel 29-arbetsgruppen ger personuppgiftsbiträdet en indirekt skyldighet att lämna sådan information till den personuppgiftsansvarige. När dataskyddsförordningen träder i kraft kommer dock denna skyldighet att gälla direkt för personuppgiftsbiträden. Detta framgår av dataskyddsförordningen artikel 28.2, där det anges att personuppgiftsbiträdet behöver informera den personuppgiftsansvarige om eventuella planer på att anlita nya underbiträden.

Denna informationsskyldighet ger upphov till flera praktiska frågor. Den första frågan är om ett personuppgiftsbiträde behöver invänta den ansvariges godkännande innan anlitandet av ett nytt underbiträde, eller om personuppgiftsbiträdet bara behöver informera den personuppgiftsansvariga och sedan kan anlita underbiträdet utan att invänta svar. Om artikeln ska tolkas på det första sättet uppkommer praktiska problem. Ett personuppgiftsbiträde, exempelvis en molntjänstleverantör, kan vara biträde åt tusentals personuppgiftsansvariga som använder molntjänsten. Om molntjänstleverantören vill anlita ett nytt underbiträde är det administrativt krångligt och affärsmässigt ineffektivt att behöva invänta ett godkännande från samtliga personuppgiftsansvariga innan avtalet ingås med underleverantören.

Det andra tolkningsförslaget, vilket framstår som det korrekta, blir mer effektivt eftersom information kan skickas ut elektroniskt till samtliga personuppgiftsansvariga utan att

[37] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 401
[38] Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing), s.10
[39] Korling, Fredric och Zamboni, Mauro (Red.) *Juridisk metodlära*, 1.5 u., Studentlitteratur AB, Lund, 2015, s. 127 f.

svar behöver inväntas. Administrativa svårigheter som att invänta och ta emot alla godkännanden undviks därmed. Dock uppkommer problem även med detta förslag. Vad händer exempelvis om personuppgiftsbiträdet skickar informationen, anlitar underbiträdet och sedan invänder den personuppgiftsansvariga mot anlitandet av underbiträdet? Är det då avtalet mellan personuppgiftsbiträdet och underbiträdet som får ge vika eller är det avtalet mellan personuppgiftsbiträdet och den personuppgiftsansvariga?

Artikel 29-arbetsgruppen har behandlat denna fråga vad avser förhållandet mellan kund och molntjänstleverantör enligt dagens regelverk. Arbetsgruppen menar att det i biträdesavtalet mellan dessa två parter bör finnas en klausul som innebär att den personuppgiftsansvarige alltid ska ha rätt att invända mot förändringar eller säga upp avtalet.[40] Arbetsgruppen menar alltså att det är avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet som kommer åsidosättas om inte underbiträdet godtas.

Ett problem med detta synsätt är att nekandet av ett underbiträde kan bli ett sätt för den personuppgiftsansvariga att komma ur ett affärsavtal med personuppgiftsbiträdet som kanske egentligen var tidsbestämt en längre tid framöver. Det kan alltså finnas en risk att denna bestämmelse utnyttjas klandervärt av den personuppgiftsansvarige. Att personuppgiftsbiträdet tvingas säga upp avtalet med underbiträdet framstår dock inte som ett bättre alternativ.

Observera att artikel 29-arbetsgruppens yttrande grundar sig på de regler som finns idag, när personuppgiftsbiträdet endast har en indirekt skyldighet att underrätta den personuppgiftsansvarige om underbiträden. Det framstår dock som troligt att arbetsgruppens tolkning av informationsskyldigheten kommer kunna tillämpas även på förordningens regler.

3.2.3 Följa instruktioner

Personuppgiftsbiträden har en skyldighet att följa den personuppgiftsansvarigas instruktioner vid behandling av personuppgifter. Denna skyldighet ska regleras i biträdesavtalet men framgår även direkt av dataskyddsdirektivet artikel 16 och 30 § 1 st. personuppgiftslagen. Det framgår inte av direktivet eller personuppgiftslagen vad instruktionerna ska innehålla, men eftersom det är den personuppgiftsansvariges ansvar enligt 9 § personuppgiftslagen att se till att personuppgifterna behandlas bara om det är lagligt, på ett korrekt sätt och i enlighet med god sed är utgångspunkten att instruktionerna ska vara så tydliga att även behandling utfört av ett personuppgiftsbiträde uppfyller dessa krav.

[40] Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing), s. 20

Personuppgiftsbiträdet ska även veta för vilket ändamål uppgifterna behandlas och till vem som uppgifterna får lämnas ut. Att biträden endast får behandla personuppgifter på den personuppgiftsansvariges instruktioner kan även anses innebära en tystnadsplikt.[41] Denna tystnadsplikt behandlas i ett särskilt avsnitt nedan i kap 3.2.4. Skyldigheten att följa instruktioner kommer inte förändras utan den återfinns i dataskyddsförordningen artikel 29.

3.2.4 Vidta tystnadsplikt

Ovan nämner framställningen att personuppgiftsbiträdet kan ha en skyldighet att vidta tystnadsplikt. Denna tystnadsplikt ska i så fall anses ingå i skyldigheten att följa den personuppgiftsansvariges instruktioner, eftersom biträdet inte utan instruktioner från den personuppgiftsansvarige får lämna uppgifter till en tredje part. Om så är fallet ska skyldigheten att vidta sekretess anses framgår av dataskyddsdirektivet artikel 16 samt 30 § 1–2 st. personuppgiftslagen. Att dataskyddsdirektivet artikel 16 benämns ”Sekretess och säkerhet vid behandling” tyder på att en sådan skyldighet ska anses ingå i skyldigheten att följa instruktioner. Denna skyldighet anses dessutom innebära att personuppgiftsbiträdet måste se till att de som arbetar under personuppgiftsbiträdet (underbiträden eller medhjälpare) också vidtar tystnadsplikt.[42]

EU har dock inte ansett att denna skyldighet framgått tillräckligt tydligt i skyldigheten att följa instruktioner. Det framgår nämligen av dataskyddsförordningen artikel 28.3 b) att personuppgiftsbiträdesavtalet ska innehålla en skyldighet för personuppgiftsbiträdet att se till att ”de personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt”. Oavsett om personuppgiftsbiträdet idag har en skyldighet att se till att de som arbetar under biträdet vidtar tystnadsplikt, kommer en sådan skyldighet att införas i och med dataskyddsförordningen.

3.2.5 Vidta säkerhetsåtgärder

Personuppgiftsbiträden har även en skyldighet att vidta lämpliga tekniska och organisatoriska skyddsåtgärder vid behandlingen av personuppgifter. Denna skyldighet är inte direkt författningsreglerad för personuppgiftsbiträden idag men ska enligt dataskyddsdirektivet artikel 17.3 och 30 § 2 st. personuppgiftslagen framgå av biträdesavtalet. Vilka åtgärder som anses som lämpliga beror enligt Dataskyddsdirektivet artikel 17.1 samt personuppgiftslagen 31 § på vilka tekniska möjligheter som finns, hur mycket åtgärderna kostar, vilka risker som

[41] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 432
[42] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordstedts Juridik AB, 2011, s. 432 ff.

finns med behandlingen och hur pass känsliga uppgifterna är. Hur många olika människors uppgifter som behandlas kan också påverka lämpligheten av säkerhetsåtgärder.[43]

Datainspektionen har i 32 § personuppgiftslagen bemyndigats att i enskilda fall besluta om vilka säkerhetsåtgärder som kan anses som lämpliga. Datainspektionen har även publicerat allmänna råd som behandlar detta. Några av de säkerhetsåtgärder som Datainspektionen anser vara lämpliga är; fysiskt skydd för IT-utrustningen, behörighetskontroll, logg för behandlingshistorik, tydlig säkerhetspolicy, tydliga rutiner, säkerhetskopiering, kryptering, antivirusprogram m.m.[44] Detta är alltså exempel på några av de skyddsåtgärder som bör vidtas av såväl personuppgiftsansvarig och personuppgiftsbiträden. Observera att detta endast är allmänna rekommendationer och därmed inte bindande. Enligt nuvarande reglering avgörs omfattningen av denna skyldighet genom en avvägning av samtliga omständigheter.

Skyldigheten att vidta lämpliga skyddsåtgärder ändras genom att skyldigheten får författningsstöd även vad gäller biträden och således inte endast kommer regleras genom avtal. Skyldigheten kommer finnas reglerad i dataskyddsförordningen artikel 32. Artikeln ger även exempel på vad som kan vara lämpliga skyddsåtgärder, något som tidigare lämnats åt medlemsstaterna att avgöra. Bland annat nämner förordningen i artikel 32 pseudonymisering[45], kryptering och säkerhetskopiering av personuppgifter som lämpliga skyddsåtgärder.

Som ytterligare vägledning till vad som anses som en lämplig säkerhetsåtgärd kan biträdet följa den Europeiska dataskyddsstyrelsens riktlinjer.[46] Reglerna kring denna styrelse återfinns i dataskyddsförordningen artikel 68. Styrelsen kommer enligt artikeln bestå av chefen för en tillsynsmyndighet per medlemsstat samt av den Europeiska datatillsynsmannen eller respektive företrädare. Styrelsens uppgifter är enligt artikel 70 bland annat att utfärda riktlinjer och rekommendationer av olika slag. Biträdet kan även följa eventuellt dataskyddsombuds anvisningar för att få vägledning till vad som är en lämplig säkerhetsåtgärd.[47] Vad som menas med ett dataskyddsombud beskrivs nedan i kap 3.3.2.

[43] SOU 1997:39 s. 412
[44] Datainspektionens allmänna råd – Säkerhet för personuppgifter, Stockholm, reviderad version november 2008.
[45] Pseudonymisering är enligt Artikel 29-arbetsgruppens yttrande 05/2014 om avidentifieringsmetoder antaget den 10 april 2014, s. 20 ff., en säkerhetsmetod som innebär att man ersätter ett attribut i en text, t.ex. ett namn, med något annat.
[46] Dataskyddsförordningen, skäl 77
[47] Dataskyddsförordningen, skäl 77

3.3 Nya skyldigheter enligt dataskyddsförordningen

3.3.1 Underrättelse av personuppgiftsincident

Förordningen innebär inte bara en förändring av nuvarande skyldigheter, utan förordningen innebär även att helt nya skyldigheter påförs personuppgiftsbiträden. En sådan ny skyldighet återfinns i artikel 33.2, nämligen personuppgiftsbiträdets skyldighet att utan onödigt dröjsmål underrätta den personuppgiftsansvarige om det sker en personuppgiftsincident. När den personuppgiftsansvarige underrättats om incidenten ska den personuppgiftsansvarige anmäla detta till Datainspektionen.

Med en personuppgiftsincident menas enligt dataskydds-förordningen artikel 4.12 ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”. Det är viktigt att en anmälan sker eftersom en personuppgifts-incident kan leda till skada för den registrerade. Exempel på situationer som kan uppstå om personuppgifter behandlas på fel sätt eller av fel person är att den registrerade kan råka ut för identitetsstöld, bedrägeri, ekonomisk förlust, skadat anseende m.m.[48]

En underrättelse om en personuppgiftsincident ska som sagt ske ”utan onödigt dröjs-mål”. Frågan är vad som menas med detta uttryck, hur lång tid har ett personuppgiftsbiträde på sig att underrätta den personuppgiftsansvariga innan konsekvenser kan inträda? Enligt förordningens skäl 87 bör frågan om en underrättelse lämnats ”utan onödigt dröjsmål” avgöras med hänsyn till incidentens art, svårighetsgrad, följder och negativa effekter för den registrerade. Det lämnas dock osagt vilka tidsramar det borde röra sig om.

Viss ledning kan hämtas av situationen när en personuppgiftsincident sker hos den personuppgiftsansvariga. I detta fall ska den personuppgiftsansvarige enligt förordningens artikel 33.1 göra en anmälan till Datainspektionen inom 72 timmar. En sådan anmälan ska innehålla särskild information som räknas upp i artikel 33.3. Bland annat ska anmälan inne-hålla information om antal registrerade som berörs, hur många och vilka uppgifter som röjts, vilka sannolika konsekvenser som kan uppkomma, vilka åtgärder som företaget planerar att vidta m.m.

En anmälan kräver således en del arbete från den personuppgiftsansvariges sida, till skillnad från vad som krävs av personuppgiftsbiträdet för att uppfylla sin skyldighet. Eftersom

[48] Dataskyddsförordningen, skäl 85

den personuppgiftsansvarige har 72 timmar på sig att göra en anmälan, kan tänkas att ett personuppgiftsbiträde bör vara skyldigt att underrätta den personuppgiftsansvarige fortare än så. Det bör dock uppmärksammas att ett personuppgiftsbiträde, exempelvis Microsoft, kan vara ett biträde för många företag. Att underrätta samtliga personuppgiftsansvariga vars uppgifter biträdet behandlar kan således medföra en del arbete. Om personuppgiftsbiträdet har ett register över samtliga personuppgiftsansvariga och deras kontaktuppgifter, bör det dock med elektroniska hjälpmedel kunna ske en underrättelse förhållandevis enkelt. Ett sådant register är personuppgiftsbiträdet skyldig att upprätta enligt dataskyddsförordningen artikel 30.2, se nedan under kap 3.3.3.

När en anmälan görs kan åtgärder vidtas för att minska skaderisken eller skadeeffekten för den registrerade. Det är således viktigt att den personuppgiftsansvarige får information om en personuppgiftsincident. Att denna skyldighet införs för personuppgiftsbiträden är således inget konstigt, speciellt inte när man jämför den registrerades intresse av att en anmälan görs och det som krävs av biträdet för att underrätta den ansvarige.

3.3.2 Utse dataskyddsombud

Ytterligare en skyldighet som personuppgiftsbiträdena i vissa fall måste uppfylla är att utse ett dataskyddsombud. I direktivet och personuppgiftslagen beskrivs begreppet som uppgiftskyddsombud samt personuppgiftsombud. Dessa begrepp har samma betydelse och kommer nedan beskrivas gemensamt under namnet dataskyddsombud, vilket är dataskyddsförordningens benämning av begreppet.

Definitionen av ett dataskyddsombud lyder enligt personuppgiftslagen 3 § ”Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt”. Ett dataskyddsombud ska alltså kontrollera att den personuppgiftsansvariga följer lagen. Ett dataskyddsombud kan vara en anställd eller en utomstående person. Ombudets skyldigheter framgår av dataskyddsdirektivet 18.2 samt 38–39 §§ personuppgiftslagen. Ombudet ska enligt dessa lagrum påpeka brister för den personuppgiftsansvarige, föra ett register över den behandling som görs samt i vissa fall anmäla den personuppgiftsansvarige till tillsynsmyndigheten. Personuppgiftslagen föreskriver i 40 § även ytterligare en skyldighet för ombudet, nämligen att hjälpa registrerade att få rättelse. Anledningen till varför vissa personuppgiftsansvariga utser ett dataskyddsombud idag är att de då kan slippa den annars obligatoriska anmälningsplikt som krävs enligt direktivets artikel 18.1 samt 36 § personuppgiftslagen. Det är dock idag helt frivilligt att utse ett dataskyddsombud.

Detta kommer att ändras när dataskyddsförordningen träder ikraft. Det kommer i vissa fall att bli obligatoriskt med ett dataskyddsombud. Denna skyldighet kommer gälla såväl personuppgiftsbiträdet som den personuppgiftsansvarige. I Kommissionens förslag, som ligger till grund för dataskyddsförordningen, anges i artikel 35 att företag med mindre än 250 anställda inte skulle behöva utse ett dataskyddsombud.[49] Denna undantagsregel har dock borttagits i den slutliga versionen av dataskyddsförordningen. Skyldigheten att utse ett dataskyddsombud gäller således alla företag som uppfyller de kriterier som framställningen nämner nedan. Ett dataskyddsombuds uppgifter ska enligt dataskyddsförordningen artikel 39 bestå av att bland annat informera och ge råd till företaget, övervaka företagets efterlevnad av förordningen, samarbeta med tillsynsmyndigheten m.m.

Personuppgiftsbiträdet ska enligt dataskyddsförordningen artikel 37 utse ett dataskyddsombud i två olika fall. Det första fallet rör själva behandlingen. Om företagets kärnverksamhet utgör en behandling som kräver att de registrerade i stor omfattning utför en regelbunden och systematisk övervakning av behandlingen, ska företaget utse ett dataskyddsombud.

Det andra fallet rör själva personuppgifterna. Om företagets kärnverksamhet innebär att behandla personuppgifter som tillhör en särskild kategori av uppgifter eller består av uppgifter om fällande domar i brottmål och överträdelser, ska företaget också utse ett dataskyddsombud. Med behandling av särskilda kategorier av uppgifter menas enligt dataskyddsförordningen artikel 9 personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller en fysisk persons sexuell läggning. Kategorin innefattar även uppgifter om en fysisk persons sexualliv eller hälsa samt biometriska eller genetiska uppgifter.

Vad som kan diskuteras är framförallt hur det första fallet angående själva behandlingen ska tolkas i praktiken. Vilken behandling kräver att den registrerade utför en regelbunden och systematisk övervakning? Regeln lämnar utrymme för att företag kan dra olika slutsatser angående deras skyldighet att utse ett personuppgiftsombud. Om ett företag drar en felaktig slutsats angående sin skyldighet kan det få betungande konsekvenser. Vid osäkerhet kan det således vara tryggare att utse ett dataskyddsombud än att inte göra det.

[49] Europeiska Kommissionens förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och
om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), COM(2012) 11 final

3.3.3 Föra skriftligt register och samarbeta med Datainspektionen

Det finns idag ingen fastställd skyldighet för personuppgiftsbiträden att föra ett register över sin personuppgiftsbehandling. Däremot finns det en indirekt skyldighet att föra ett sådant register. Detta framgår av artikel 29-arbetsgruppens yttrande om datormoln, där arbetsgruppen angett riktlinjer för personuppgiftsansvariga och personuppgiftsbiträden. Arbetsgruppen anger att det i biträdesavtalet bör framgå en skyldighet för personuppgiftsbiträdet att uppge samtliga av sina underleverantörer. Personuppgiftsbiträdet har även enligt arbetsgruppen en skyldighet att informera den personuppgiftsansvarige om var personuppgiftsbehandlingen sker (inklusive var underleverantörerna utför personuppgiftsbehandlingen) samt de tekniska och organisatoriska åtgärder som leverantören vidtagit.[50] Dessa riktlinjer är inte bindande, men kan ha en bindande karaktär. Bland annat läggs de ibland till grund för Datainspektionens tillsynsärenden.[51]

I och med att personuppgiftsbiträden har en skyldighet att informera den personuppgiftsansvarige om samtliga underleverantörer och den behandling som sker, kan det ses som en indirekt skyldighet att ha ett register innehållande denna information. Annars blir det svårt att kunna tillhandahålla informationen.

Oavsett om det idag finns en skyldighet att föra ett register över underbiträden, eller endast en informationsskyldighet, kommer det finnas en fastställd skyldighet för personuppgiftsbiträden att föra ett register över sin behandling när dataskyddsförordningen träder ikraft. Skyldigheten återfinns i artikel 30.2-4. Registret ska innehålla kontaktuppgifter till personuppgiftsbiträdet, underbiträden, samtliga personuppgiftsansvariga samt eventuella företrädare och dataskyddsombud. Registret ska även innehålla information om vilka behandlingar som utförs, eventuella tredjelandsöverföringar samt om möjligt de lämpliga tekniska och organisatoriska säkerhetsåtgärder som personuppgiftsbiträdet vidtagit.

Personuppgiftsbiträdet är även skyldigt att på begäran lämna ut registret till medlemsstatens tillsynsmyndighet, vilken för Sveriges del är Datainspektionen. Syftet med att personuppgiftsbiträden ska lämna registret till Datainspektionen är för att det ska underlätta myndighetens övervakning av behandlingen.[52] Denna skyldighet gäller enligt dataskyddsförordningen artikel 30.5 inte för företag som sysselsätter färre än 250 personer, såvida inte den behandling som utförs sannolikt kommer medföra en risk för de registrerades fri och rättigheter, behandlingen inte är tillfällig, behandlingen omfattar sådana särskilda kategorier av uppgifter som

[50] Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing), s. 20
[51] DI 1475-2013 (2014-04-25)
[52] Dataskyddsförordningen skäl 82

beskrivits i ovan i kapitel 3.3.2. eller personuppgifter om fällande domar i brottmål eller överträdelser.

Skyldigheten att föra ett register kan medföra praktiska utmaningar. För exempelvis en molntjänstleverantör som har många kunder kan det vara tidskrävande att kartlägga alla kunder, deras kontaktpersoner och dataskyddsombud samt utreda vilka kategorier av behandlingar som utförs för varje enskild kund. Det ställs sedan som krav att personuppgiftsbiträdet anger om personuppgifter kommer överföras till tredje land. Om personuppgiftsbiträdet använder sig av underbiträden, måste personuppgiftsbiträdet således även utreda om underbiträdena använder sig av exempelvis servrar i tredje land. Detta kan bli omfattande om personuppgiftsbiträdet har många underbiträden. Eftersom bestämmelsen riktar sig till större företag, närmare bestämt de som har över 250 anställda, kan tänkas att företagen kommer ha både många personuppgiftsansvariga och underbiträden att kartlägga vid upprättandet av registret.

Personuppgiftsbiträdet ska även *om möjligt* göra en allmän beskrivning av de tekniska och organisatoriska åtgärder som vidtas. Frågan är vad som menas med uttrycket ”om möjligt”. Hur svårt ska det vara att överskåda åtgärderna för att biträdet ska slippa lämna en sådan beskrivning?

En annan skyldighet för biträden återfinns i artikel 31. Denna skyldighet innebär att personuppgiftsbiträdet, utöver att lämna ett sådant register som beskrivits ovan, på begäran ska samarbeta med Datainspektionen vid utförandet av tillsynsmyndighetens uppgifter. Tillsynsmyndighetens uppgifter är många och återfinns i dataskyddsförordningen artikel 57. En av uppgifterna innebär att hantera klagomål från registrerade. För att kunna utreda sakfrågan kan tänkas att myndigheten behöver information från ett personuppgiftsbiträde, om klagomålet rör en behandling som biträdet utfört. Detta skulle kunna vara ett exempel på när ett personuppgiftsbiträde är skyldigt att samarbeta med Datainspektionen.

3.3.4 Möjliggöra och bidra till granskningar av den personuppgiftsansvarige

I dataskyddsdirektivet artikel 17.2 anges att den personuppgiftsansvarige ska välja ett personuppgiftsbiträde som kan ge tillräckliga garantier för de tekniska och organisatoriska säkerhetsåtgärder som måste vidtas samt ”tillse att dessa åtgärder genomförs”. Denna regel har implementerats i 31 § 2 st. personuppgiftslagen, där det anges att den personuppgiftsansvarige på samma sätt som i direktivet ska tillse att biträdet kan genomföra de säkerhetsåtgärder som krävs samt ”se till att personuppgiftsbiträdet verkligen vidtar åtgärderna”. Det finns således en skyldighet för den personuppgiftsansvarige att kontrollera personuppgiftsbiträdet. Det framgår

dock inte hur denna kontroll ska vidtas och reglerna föreskriver inte heller några skyldigheter för personuppgiftsbiträdet vad gäller denna kontroll.

I dataskyddsförordningen artikel 28.3 h) 1 st. införs dock en avtalsrättslig skyldighet för personuppgiftsbiträden. Skyldigheten innebär att personuppgiftsbiträdet ska ”ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige”. Det införs således en ny skyldighet för biträden som innebär informationslämnande samt bidragande till granskningar.

Enligt dataskyddsförordningen artikel 28.3 h) 2 st. inkluderar denna skyldighet även att personuppgiftsbiträdet omedelbart ska ”informera den personuppgiftsansvarige om han anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser”. En aktuell fråga här är hur uttrycket ”han anser” ska tolkas. Betyder detta att personuppgiftsbiträdet har en skyldighet att alltid kontrollera och jämföra de instruktioner som den personuppgiftsansvarige lämnar med förordningen och på så sätt avgöra om han (biträdet) anser att instruktionerna strider mot förordningen? I så fall kan sägas att biträdet även har ett kontrollansvar gentemot den personuppgiftsansvarige.

3.3.5 Bistå i konsekvensbedömning och förhandssamråd

Utöver de skyldigheter som nämnts ovan har personuppgiftsbiträdet enligt artikel 38.3 f) en avtalsenlig skyldighet att bistå den personuppgiftsansvarige att uppfylla dennes skyldigheter vad gäller konsekvensbedömning samt förhandssamråd. Med konsekvensbedömning menas enligt dataskyddsförordningen artikel 35 att det utförs en bedömning av den planerade behandlingens konsekvenser. En sådan bedömning ska innehålla en beskrivning av den planerade behandlingen, behandlingens syften och om lämpligt den personuppgiftsansvariges berättigande intressen. Bedömningen ska även innehålla en proportionalitetsbedömning av behandlingen jämfört med syftena, en bedömning av de risker med avseende på de registrerades fri- och rättigheter som behandlingen kan innebära samt vilka åtgärder som kommer vidtas för att skydda personuppgifterna.

Exakt hur personuppgiftsbiträdet ska bistå den personuppgiftsansvariga i konsekvensbedömningen framgår inte av förordningen. Eftersom det i vissa fall är personuppgiftsbiträdet som utför hela behandlingen, förefaller det dock i många fall naturligt att biträdet vet mer än den personuppgiftsansvarige om exempelvis vilka tekniska skyddsåtgärder som kommer vidtas. I dessa fall ska alltså biträdet bistå den personuppgiftsansvarige med sådan

information. Utöver att bistå den personuppgiftsansvarige i dennes konsekvensbedömning, bör personuppgiftsbiträdet även göra en riskutvärdering för egen del. Detta framgår av skäl 83 till förordningen, där det framgår att personuppgiftsbiträdet ska utvärdera de risker som finns med behandlingen och vidta åtgärder för att minska sådana risker.

Om den personuppgiftsansvariges konsekvensbedömning visar stora risker med behandlingen, ska den ansvarige innan behandlingen börjar samråda med tillsynsmyndigheten. Detta kallas ett förhandssamråd och återfinns i dataskyddsförordningen artikel 36. Under samrådet ska den personuppgiftsansvarige i stort sett lämna den information till tillsynsmyndigheten som samlades in under konsekvensbedömningen. Om den personuppgiftsansvarige vid samrådet behöver mer uppgifter från personuppgiftsbiträdet, ska biträdet bistå den ansvarige med sådan information.

3.3.6 Återföring och radering av personuppgifter

Det finns idag ingen författningsreglerad skyldighet för personuppgiftsbiträden att radera eller återlämna personuppgifter till den personuppgiftsansvarige. Denna skyldighet bör dock enligt artikel 29-arbetsgruppen regleras i avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet.[53]

När dataskyddsförordningen träder ikraft blir det obligatoriskt att reglera radering eller återlämning av personuppgifter för personuppgiftsbiträden i biträdesavtalet. Enligt dataskyddsförordningen artikel 28.3 g) ska avtalet reglera att personuppgiftsbiträdet, när behandlingen avslutas för den personuppgiftsansvariges räkning, raderar eller återlämnar personuppgifterna. Undantag från skyldigheten kan göras om det finns en unionsrättslig eller nationell legal skyldighet att bevara personuppgifterna, t.ex. för bokföringssyfte.

Att ha ett krav på att samtliga personuppgifter ska raderas kan ställa till problem. Personuppgifterna kan nämligen finnas i flera olika system hos personuppgiftsbiträdet och det kan vara svårt att lokalisera alla personuppgifter. Att ha sökfunktioner som kan lokalisera alla personuppgifter kan, enligt vissa rättsvetenskapsmän, snarare hota den personliga integriteten istället för att skydda den. Sådana sökfunktioner gör det nämligen väldigt lätt att kartlägga en person. Därför bör ett företag endast behöva använda de sök- och sammanställningsmöjligheter som företaget faktiskt och rättsligt har tillgång till. Inte ens EU-rätten bör kunna framtvinga det som i praktiken är omöjligt.[54]

[53] Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing), s. 12
[54] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar*, fjärde uppl., Stockholm, Nordstedts Juridik AB, 2011, s. 403

Ytterligare ett problem finns angående radering eller återlämning av uppgifter när det kommer till användningen av säkerhetskopiering (backup) hos personuppgiftsbiträden. En backup är en kopia av t.ex. en datafil som kan användas för att återskapa originalversionen om denna har skadats eller förlorats.[55] Enligt artikel 29-arbetsgruppen omfattar radering även uppgifter som finns på en backup.[56] Att radera personuppgifter från en backup kan vara problematiskt eftersom många system för säkerhetskopiering inte tillåter att data raderas utan oskäliga arbetsinsatser.[57] Det kan till och med vara praktiskt omöjligt att radera viss data på säkerhetskopiorna och leverantören kan då inte uppfylla sin skyldighet. En lösning på problemet kan vara att inhämta samtycke från de registrerade att få spara uppgifterna så länge som säkerhetskopian sparas.[58] En annan lösning är att ha korta backupcykler.[59]

[55] Nationalencyklopedin, backup. http://www.ne.se.ezp.sub.su.se (hämtad 2016-12-14)
[56] Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing), s. 12
[57] Christner, Anders och Edvardsson, Tobias, *Cloud Computing – en handledning och kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010*, 2011, s. 107
[58] Christner, Anders och Edvardsson, Tobias, *Cloud Computing – en handledning och kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010*, 2011, s. 21
[59] Christner, Anders och Edvardsson, Tobias, *Cloud Computing – en handledning och kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010*, 2011, s. 108

4. Förändrade sanktioner

4.1 Inledning

I tidigare kapitel har redogjorts för vem som är ett personuppgiftsbiträde samt hur personuppgiftbiträdets skyldigheter kommer att förändras när förordningen träder i kraft. Detta kapitel ska behandla vad som kan inträda när personuppgiftsbiträdet inte uppfyller sina skyldigheter – nämligen sanktioner. Framställningen nedan beskriver hur dessa sanktioner fungerar idag, hur de kommer att förändras i och med förordningen samt analyserar dessa förändringar.

4.2 Tillsynsmyndighetens sanktioner

Enligt dataskyddsdirektivet artikel 24 är det är upp till medlemsstaterna att besluta om de sanktioner som ska inträda om skyldigheterna inte uppfylls. För Sveriges del regleras dessa sanktioner i personuppgiftslagen, bland annat tillsynsmyndighetens befogenhet att utfärda vite. Tillsynsmyndigheten i Sverige är Datainspektionen. För det första kan Datainspektionen enligt 44 § personuppgiftslagen använda vite för att framtvinga tillräckliga underlag för sin tillsyn. Datainspektionen kan nämligen vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på annat sätt än genom lagring tills begärda underlag inkommit till myndigheten. Vad som menas med lagring i detta fall är i princip att inga åtgärder alls får vidtas med personuppgifterna men de behöver inte raderas.[60] För att Datainspektionen ska kunna tvinga en personuppgiftsansvarig att radera personuppgifter, det vill säga även förbjuda lagring, krävs enligt 47 § att Datainspektionen får ett godkännande om detta från förvaltningsrätten.

Den andra situationen där vite kan förekomma är om Datainspektionen konstaterar att personuppgifter behandlas eller kan komma att behandlas olagligt. Innan Datainspektionen använder vite som ett påtryckningsmedel ska myndigheten med påpekanden eller liknande förfaranden försöka få den personuppgiftsansvarige att vidta rättelse. Om inte rättelse vidtas, eller om ärendet är brådskande, kan Datainspektionen enligt 45 § 1 st. vid vite förbjuda all annan behandling än lagring. Myndigheten kan även enligt 45 § 2 st. utfärda vite om inte en personuppgiftsansvarig följer ett sådant beslut om lämpliga säkerhetsåtgärder som beskrivits ovan i kapitel 3.2.5. Innan Datainspektionen beslutar om vite ska den personuppgiftsansvarige enligt 46 § få tillfälle att yttra sig.

[60] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar*, fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 499 f.

Ett vitesbelopp ska enligt 3 § lagen (1985:206) om viten bestämmas med hänsyn till adressatens ekonomiska förhållanden och omständigheterna i övrigt. Ungefär vilket belopp, exempelvis en viss procentsats av årsinkomsten, det skulle kunna röra sig om är oklart eftersom Datainspektionen aldrig förelagt om vite. Det finns således ingen myndighetspraxis på området.[61]

På vissa områden i svensk rätt har myndigheter en befogenhet att påföra sanktionsavgifter. Exempel på svensk lagstiftning som innehåller regler om sanktionsavgifter kan nämnas produktsäkerhetslag (2004:451), som bygger på ett EU-direktiv.[62] Även marknadsföringslag (1995:450) samt konkurrenslag (1993:20) är sådana exempel. [63]

En sanktionsavgift är en bestraffande avgift som kan utfärdas till en juridisk person som redan brutit mot regler.[64] Detta skiljer sig från viten som endast är ett hot om att betalningsansvar kan uppstå om företaget inte ändrar sitt beteende i framtiden.[65] I personuppgiftslagen finns det inte några möjligheter för tillsynsmyndigheten att utfärda sanktionsavgift om ett företag bryter mot regler om personuppgiftsskydd. Detta kommer dock införas i dataskyddsförordningen.

Enligt dataskyddsförordningen artikel 58, som behandlar tillsynsmyndighetens befogenheter, anges i andra stycket punkten i) att tillsynsmyndigheten ska ha befogenhet att påföra administrativa sanktionsavgifter. En sådan sanktionsavgift ska enligt artikeln påföras *utöver* eller *istället för* de befogenheterna som annars uppräknas i det stycket. Bland dessa befogenheter återfinns bland annat myndighetens möjlighet att utfärda varning eller reprimand.

Myndighetens befogenhet att varna ett företag kan tyckas likna det vitesförfarande som finns i personuppgiftslagen idag, som innebär att företag ska kunna vidta rättelse. Dock kan myndigheten enligt artikel 58.2 a) endast varna om att *planerade* behandlingar sannolikt kommer bryta mot förordningen. Det har i dessa fall inte skett någon felaktig behandling än. När tillsynsmyndigheten uppmärksammar att en behandling redan bryter mot förordningen kan myndigheten enligt artikel 58.2 b) utfärda reprimander. En reprimand ska dock utfärdas istället för en administrativ sanktionsavgift endast vid mindre överträdelser eller om en sanktionsavgift skulle innebära en oproportionerlig börda för en *fysisk* person.[66] I annat fall kan en reprimand kombineras med en sanktionsavgift.

[61] Vad är straffbart enligt personuppgiftslagen? – En vägledning från Datainspektionen för polis och åklagare, Januari 2011, s. 32
[62] Europaparlamentet och Rådets Direktiv 2001/95 EG av den 3 december 2001 om allmän produktsäkerhet
[63] Prop. 1981/82:142 s. 4
[64] Prop. 1981/82:142 s. 6
[65] Prop. 2003/04:121 s. 146
[66] Dataskyddsförordningen skäl 148

Andra befogenheter som räknas upp i artikel 58.2 är tillsynsmyndighetens möjlighet att utfärda förelägganden i olika sammanhang, att begränsa eller förbjuda viss personuppgiftsbehandling eller att återkalla en certifiering. Eftersom en sanktionsavgift kan kombineras med dessa befogenheter kan en avgift exempelvis påföras även om ett företag efter ett föreläggande ändrar sitt beteende. På så sätt blir tillsynsmyndighetens rättsmedel mer effektivt och avskräckande än tidigare och till skillnad från hur det ser ut idag med vitesreglerna har sanktionsavgifterna en större möjlighet att realiseras.

Utöver det förhållandet att sanktionsavgifterna antagligen kommer blir mer effektiva än viten, är sanktionsavgifterna även avskräckande eftersom avgifterna består av höga belopp. Reglerna om de administrativa sanktionsavgifterna återfinns i dataskyddsförordningen artikel 83 och beskriver två olika beloppskategorier. Den första kategorin återfinns i artikelns fjärde stycke och anger att sanktionsavgiften kan uppgå till 10 000 000 EUR eller 2 % av ett företags totala globala årsomsättning, beroende på vilket värde som är högst. Detta belopp kan ett företag behöva betala om företaget inte uppfyller de skyldigheter som uppräknades ovan i kapitel 3.

Den andra beloppskategorin återfinns i artikelns femte stycke och anger en övre beloppsgräns på 20 000 000 EUR eller 4 % av den totala globala årsomsättningen. Detta belopp kan ett företag behöva betala om behandlingen strider mot förordningens grundläggande principer (som uppräknas i artikel 5), om det saknas laglig grund för behandlingen, om den registrerade inte får sina rättigheter tillgodosedda, om det sker en olaglig överföring av uppgifter till tredje land, om företaget inte rättar sig efter tillsynsmyndighetens föreläggande m.m. Det är således höga sanktionsavgifter som kan bli aktuella om reglerna i förordningen inte följs.

Dessa höga belopp är dock den övre gränsen för vad en sanktionsavgift enligt dataskyddsförordningen kan uppgå till. Storleken på beloppet kan variera i varje enskilt fall. Vad som kan påverka beloppets storlek räknas upp i artikel 83.2 – exempelvis; antalet berörda registrerade, den skada de registrerade har lidit, om överträdelsen skett genom uppsåt, eventuella tidigare överträdelser, de åtgärder som vidtagits för att minska skadan, de lämpliga tekniska och organisatoriska säkerhetsåtgärder som genomförts i förebyggande syfte, m.m. Framförallt det sista exemplet visar på vikten av att företagen redan nu börjar arbeta för att verksamheten ska uppfylla alla de krav som förordningen ställer. Även om inte alla brister hinner åtgärdas innan den 25 maj 2018, kan ett påbörjat åtgärdsarbete minska den eventuella sanktionsavgift som företaget kan komma att påföras.

Att förordningen ger tillsynsmyndigheten befogenhet att utfärda administrativa sanktionsavgifter behöver dock inte betyda att tillsynsmyndigheten inte kommer kunna utfärda viten. Enligt förordningens artikel 84 ska medlemsstaterna själva fastställa regler om ytterligare sanktioner för överträdelser av denna förordning. Regeringen har gett Dataskyddsutredningen (Ju 2016:04) i uppdrag att analysera vilka dessa regler skulle kunna bli. Utredningen ska redovisa sin analys senast den 12 maj 2017.[67] Det kan alltså hända att utredningen kommer fram till att vitesreglerna ska finnas kvar, parallellt med sanktionsavgifterna.

Förordningen uttrycker dock i artikel 84 att dessa sanktioner särskilt ska gälla för de överträdelser som inte omfattas av administrativa sanktionsavgifter. Även i svensk lagstiftning är man restriktiv till att utdöma dubbla ekonomiska sanktioner. I produktsäkerhetslagen, marknadsföringslagen samt konkurrenslagen, som alla innehåller bestämmelser om sanktionsavgifter, har det tagits in en uttrycklig bestämmelse om att sanktionsavgifterna inte ska kombineras med vite.[68] Mycket talar därför för att utredningen kommer komma fram till att tillsynsmyndigheten inte ska kunna kombinera vite och sanktionsavgifter.

Idag får företagen en chans att rätta till sina överträdelser innan vite utdöms, något som inte kommer vara möjligt när förordningen träder ikraft. Att företagen får en chans att rätta sina misstag innan de behöver betala ett vitesbelopp kan anses rimligt. Detta förfarande kan dock medföra problem. Istället för att företagen använder sina resurser till att själva kartlägga sin verksamhet och upptäcka eventuella brister som måste åtgärdas, kan de vänta tills Datainspektionen gör det åt dem. Företagen tjänar således tidsmässigt och ekonomiskt på att strunta i de regler som finns. För att personuppgiftsskyddet ska stärkas är det därför rimligt att tillsynsmyndigheten kan använda sig av effektiva sanktioner. Det återstår att se hur Datainspektionen kommer hantera befogenheten att utdöma sanktionsavgifter. Antingen kommer myndigheten ta på sig en sträng roll, eller så kommer myndigheten endast utdela reprimander genom att använda sig av undantaget ”mindre överträdelser” och således undvika att dela ut betungande sanktionsavgifter.

4.3 Skadestånd

En annan sanktion som kan bli tillämplig om kravet på personuppgiftsskydd inte uppfylls är skadestånd. Som kommer framgå nedan skiljer sig skadeståndet enligt nuvarande regler och

[67] SOU 2016:58 s. 382
[68] Prop. 2003/04:121 s. 162

kommande regler inte särskilt mycket åt. Detta innebär att mycket av det som gäller idag angående själva skadeståndet fortfarande kommer gälla när förordningen träder i kraft. Dock kommer personuppgiftsbiträden kunna bli direkt skadeståndsskyldiga, vilket gör att det ändå är viktigt för framställningen att belysa vad skadeståndet innebär och kommer att innebära.

I dataskyddsdirektivet artikel 23 1 st. föreskrivs att medlemsstaterna ska reglera att den som lidit skada till följd av en felaktig personuppgiftsbehandling ska få ersättning av den personuppgiftsansvarige. Sverige har implementerat denna regel i 48 § 1 st. personuppgiftslagen, där det förskrivs följande: ”Den personuppgiftsansvarige skall ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag har orsakat.”

Med skada enligt 48 § personuppgiftslagen avses såväl personskada, sakskada som ren förmögenhetsskada.[69] Även om ingen ekonomisk skada uppstår kan den registrerade få ersättning på grund av den kränkning av den personliga integriteten som lagbrottet medfört (ideell skada). Skadeståndsansvaret är strikt, vilket innebär att det inte uppställs som krav att den ansvarige ska ha agerat med uppsåt eller oaktsamhet för att skadeståndet ska inträda.[70] För skadeståndsansvar krävs att det finns ett adekvat orsakssamband mellan den olagliga behandlingen och skadan och/eller kränkningen som uppstått.[71]

Personuppgiftslagens bestämmelser om skadestånd har företräde framför de allmänna reglerna i skadeståndslag (1972:207). Detta framgår av 1 kap 1 § skadeståndslagen, där det anges att skadeståndslagen är sekundär i förhållande till annan rätt. Att personuppgiftslagen har företräde framför skadeståndslagen har betydelse eftersom skadeståndsansvaret enligt de båda lagarna skiljer sig åt i vissa avseenden. En sådan skillnad är att personuppgiftslagen ger rätt till ersättning för ren förmögenhetsskada och kränkning utan att ett brott begåtts, vilket skiljer sig från skadeståndslagens reglering. En annan skillnad är att skadeståndsansvaret enligt skadeståndslagen inte är strikt.[72] Vissa frågor regleras dock fortfarande av de allmänna skadeståndsreglerna i skadeståndslagen, bland annat hur ersättningen ska beräknas.[73]

[69] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 513
[70] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 507
[71] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 514
[72] Prop. 2001/02:144 s. 45
[73] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 510

Storleken på skadestånd för person och sakskada beräknas enligt skadeståndslagen kapitel 5 och är väldigt varierande, eftersom det har till syfte att ersätta den ekonomiska förlust som uppstått i det enskilda fallet.[74] Vad gäller kränkningsersättningen blir beräkningen mer intressant eftersom det i dessa fall inte finns någon mätbar ekonomisk skada. Istället har vissa schablonbelopp utformats av praxis, vilket framgår av bland annat NJA 2013 s. 1046. Rättsfallet handlar om ett företags skadeståndsskyldighet enligt personuppgiftslagen 48 §, när företaget publicerat en tvistemålsdom på sin hemsida utan att radera parternas namn. En av parterna stämde företaget för att publiceringen kränkt hans personliga integritet. HD nämner i sina domskäl att ersättning för inte allvarliga kränkningar bör beräknas till under 5 000 kr och att mindre allvarliga, men inte obetydliga, kränkningar bör leda till en ersättning på 3 000 kr. Vidare finns det en stor mängd beslut från Justitiekanslern som ofta beslutar om skadestånd när en skadelidande stämmer staten för bristande personuppgiftshantering. Bland dessa beslut verkar ersättningen i de flesta fall bestämmas till 1 000 kr – 10 000 kr.[75]

Ovan har beskrivits vad skadestånd enligt personuppgiftslagen innebär idag och hur det beräknas. Som beskrivits i inledningen av detta avsnitt kommer det inte bli någon större skillnad när dataskyddsförordningen träder i kraft. I dataskyddsförordningen artikel 82 anges att varje person som lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ska ha rätt till ersättning för skadan. Materiell och immateriell skada kan beskrivas som en skada av ekonomisk natur samt skada av icke ekonomisk natur, vilket kan jämställas med personuppgiftslagens regler om ekonomisk och ideell skada.[76] Precis som i personuppgiftslagen är ersättningsskyldigheten enligt förordningen strikt, eftersom artikeln inte ställer några krav på culpa eller uppsåt för att ersättningsskyldigheten ska bli aktuell. I artikelns sjätte stycke anges att det är de nationella domstolarna som kommer ta upp mål om ersättning av detta slag. Detta innebär att det på samma sätt som idag kommer vara domstolarna som bestämmer ersättningens storlek, vilket innebär att det kommer göras med hjälp av skadeståndslagen och den praxis som finns idag. Man kan dock tänka sig att domstolarna kommer höja beloppen för kränkning eftersom EU med förordningen satt ner foten och poängterat hur viktigt skyddet av den personliga integriteten är.

[74] Hellner, Jan och Radetzki, Marcus, *Skadeståndsrätt*, 9:1 u., Nordstedts Juridik AB, Stockholm, 2014, s. 331 f.
[75] Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen – En kommentar,* fjärde uppl., Stockholm, Nordsteds Juridik AB, 2011, s. 517-522
[76]Europaparlamentet, utskottet för rättsliga frågor och den inte marknaden, Meddelande till ledamöterna nr 8/2004 Ärende: Förslag till betänkande med rekommendationer till kommissionen om ett vägledande europeiskt tabellverk över skadors inverkan på den fysiska och mentala integriteten (2003/2130(INI)).

4.4 Straff

Enligt dataskyddsdirektivet artikel 24 får medlemsstaterna själva bestämma vilka sanktioner de vill införa. Sverige har infört en straffbestämmelse i personuppgiftslagen 49 §. Denna straffbestämmelse kan endast riktas mot fysiska personer och innebär att den som bryter mot vissa angivna bestämmelser i personuppgiftslagen kan straffas med böter eller fängelse. Om denna straffbestämmelse ska finnas kvar när förordningen träder ikraft är, på samma sätt som angående viten, än så länge oklart.

5. Förändrad ansvarsfördelning

5.1 Inledning

I tidigare kapitel har förklarats vilka skyldigheter ett personuppgiftsbiträde har samt *vilka* sanktioner som kan inträda om biträdet inte uppfyller sina skyldigheter. I detta kapitel behandlas frågan om *när* personuppgiftsbiträdet kan drabbas av en sådan sanktion, det vill säga hur ansvarsfördelningen ser ut mellan den personuppgiftsansvarige samt personuppgiftsbiträdet. Framställningen diskuterar i slutet av varje avsnitt om den nya ansvarsfördelningen kommer kunna påverkas av avtal.

5.2 Förändrat ansvar för tillsynsmyndighetens sanktioner

Idag kan som beskrivits i kap 4.2 tillsynsmyndigheten utfärda vite. Vitesbestämmelserna i 44 – 45 §§ personuppgiftslagen riktar sig direkt till den personuppgiftsansvarige och något vite kan således inte riktas mot personuppgiftsbiträdet.

Vad gäller de administrativa sanktionsavgifterna blir situationen en annan. Detsamma gäller övriga befogenheter som uppräknats ovan under kap 4.2. Tillsynsmyndigheten har nämligen befogenhet att rikta dessa sanktioner till den personuppgiftsansvarige *och* personuppgiftsbiträdet. Detta framgår av dataskyddsförordningen artikel 58, där både den personuppgiftsansvarige och personuppgiftsbiträdet benämns som mottagare för tillsynsmyndighetens olika sanktioner. I artikelns punkt i) anges att administrativa sanktionsavgifter kan påföras utöver eller istället för de uppräknade sanktionerna. De administrativa sanktionsavgifterna och övriga sanktioner kan således riktas till både den personuppgiftsansvarige samt personuppgiftsbiträdet, vilken är en stor skillnad från hur tillsynsmyndigheten kan påverka personuppgiftsbiträden idag.

En intressant fråga är om skyldigheten att betala sanktionsavgifter skulle kunna begränsas genom avtal så att den ena parten inte kan bli betalningsskyldig, alternativt bara kan bli betalningsskyldig för en viss del. Denna fråga har nyligen behandlats i en artikel i tidskriften Lov&Data. I artikeln nämns att förordningens krav enligt artikel 83.8, nämligen att tillsynsmyndigheten ska utöva sina befogenheter på ett rättssäkert sätt, hindrar att sanktionsavgifter fördelas genom avtal. Endast den som överträtt förordningen bör kunna åläggas sanktionsavgifter.[77] Detta framstår som en rimlig slutsats.

[77] Frydlinger, David, *Ansvarsbegränsningar i biträdesavtal – relevanta eller irrelevanta under General Data Protection Regulation (GDPR)?* Lov&Data, nr. 128, häfte 4/2016, s. 34

5.3 Förändrat ansvar för skadestånd

Enligt den reglering som finns idag kan personuppgiftsbiträden inte åläggas något ansvar för skadestånd direkt baserat på dataskyddsdirektivet eller personuppgiftslagen. Det framgår nämligen av dataskyddsdirektivet artikel 23, första stycket, att den registrerade har rätt till ersättning av den *personuppgiftsansvarige*. E contrario kan skadeståndsanspråket således inte riktas mot personuppgiftsbiträdet med stöd av dataskyddsdirektivet. Enligt artikelns andra stycke framgår dock att den personuppgiftsansvarige helt eller delvis kan undgå ansvar om han bevisar att han inte är ansvarig för den händelse som orsakat skadan. Här skulle kunna tänkas att skadeståndsanspråket då istället skulle kunna riktas mot personuppgiftsbiträdet, om det är biträdet som varit orsaken till den skada som den registrerade lidit. Så är dock inte fallet. Av direktivets skäl 55 framgår att denna jämkning av skadeståndet blir tillämpligt om det är den registrerade själv som är orsakat felet, eller vid fall av force majeure. Regeln är således inte till för att fördela ett skadestånd mellan en personuppgiftsansvarig och ett personuppgiftsbiträde.

Personuppgiftslagen innebär ingen skillnad jämfört med direktivet, i 48 § personuppgiftslagen anges att ett skadeståndsanspråk ska riktas mot den personuppgiftsansvarige samt att skadeståndet kan jämkas under samma förutsättningar som anges direktivet. Om inte skadeståndet kan jämkas med stöd av personuppgiftslagen, anges i propositionen till personuppgiftslagen att skadestånd ska kunna jämkas med stöd av 6 kap 1 § skadeståndslagen. Denna paragraf reglerar dock jämkning på grund av medvållande från den registrerades sida och inte någon fördelning av skadestånd när även biträdet varit medvållande till skadan. I samma proposition framgår att något skadestånd inte kan riktas till personuppgiftsbiträden med stöd av personuppgiftslagen, det anges nämligen att ”Ett fel av t.ex. ett anlitat personuppgiftsbiträde får således anses bero på den personuppgiftsansvarige. En annan sak är att den personuppgiftsansvarige i allmänhet kan få ersättning av ett försumligt personuppgiftsbiträde för ersättning som måste betalas till registrerade”.[78]

Regeringens uttalande stödjer sig på en traditionell skadeståndsrättslig princip. Principen innebär att den som är skadeståndsskyldig på grund av strikt ansvar har full regressrätt mot den som svarar på grund av vållande. Denna traditionella princip gäller oavsett om principen framgår direkt av lag.[79] Den personuppgiftsansvariga har således full regressrätt mot personuppgiftsbiträdet även om inte detta framgår uttryckligen av personuppgiftslagen.

[78] Prop. 1997/98:44 s. 147
[79] Hellner, Jan och Radetzki, Marcus, *Skadeståndsrätt*, 8:2 u., Nordstedts Juridik AB, Stockholm, 2012 s.249 f., prop. 1972:5 s. 119 f.

Observera att regeringen i propositionen till personuppgiftslagen nämner ett *försumligt personuppgiftsbiträde* och den skadeståndsrättsliga principen uttrycker att biträdet ska vara *vållande.* För att ett biträde ska bli skadeståndsskyldigt gentemot den personuppgiftsansvarige krävs alltså att det föreligger ett visst mått av oaktsamhet från biträdets sida, det ska föreligga culpa. Bedömningen av om ett biträde varit oaktsamt kan variera från fall till fall, men som vägledning kan frågan ställas om biträdet borde ha handlat på något annat sätt.[80] Det finns alltså en skillnad mellan ansvaret för den personuppgiftsansvariga och personuppgiftsbiträdet – den personuppgiftsansvariga ansvarar strikt för alla brott mot personuppgiftslagen medan biträdet endast har ett ansvar om culpa föreligger.

Eftersom skadeståndslagen är dispositiv enligt lagens 1 kap 1 § har ett avtal mellan parterna som reglerar skadestånd företräde framför skadeståndslagen. En intressant fråga är därför om ett personuppgiftsbiträde kan påföras ett strikt skadeståndsansvar på avtalsrättsliga grunder, eller om det krävs culpa på samma sätt som i utomobligatoriska förhållanden. Denna fråga är omdiskuterad och åsikterna går isär. Vissa rättsvetenskapsmän anser att det går att avtala om strikt ansvar[81] medan andra har den har den motsatta åsikten.[82] Rättsläget är således oklart.

Personuppgiftbiträdets ansvar kommer förändras en del när dataskyddsförordningen träder ikraft. Förordningen innebär nämligen, till skillnad från dataskyddsdirektivet och personuppgiftslagen, ett strikt skadeståndsansvar även för personuppgiftsbiträden i vissa fall. I dataskyddsförordningen artikel 82.1 föreskrivs att ”Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan”.

Bestämmelsen riktar sig således både till den personuppgiftsansvarige samt personuppgiftsbiträdet. I artikel 82.2 framgår att personuppgiftsbiträdet ska ansvara endast för sådan skada som uppkommit till följd att biträdet inte uppfyllt de skyldigheter som beskrivs ovan i kap 3. Ifall både den personuppgiftsansvarige och personuppgiftsbiträdet, och i vissa fall flera biträden, medverkat till samma behandling, framgår av artikel 82.4 att de har ett solidariskt skadeståndsansvar gentemot den registrerade. Med solidariskt skadeståndsansvar menas att den registrerade kan utkräva hela skadeståndsbeloppet från endera av aktörerna, och den som

[80] Hellner, Jan och Radetzki, Marcus, *Skadeståndsrätt*, 8:2 u., Nordstedts Juridik AB, Stockholm, 2012, s.128
[81] Ramberg, Jan & Ramberg, Christina, *Allmän avtalsrätt*, 10 u., Wolters Kluwer Sverige AB, Stockholm, 2016, s. 238
[82] Bengtsson, Bertil, *Allmänna principer om kontraktsansvar*, Festskrift till Lars Gorton, 2007, s. 25

får betala beloppet får sedan regresskräva mot den/de andra iblandade.[83] Regressrätten framgår av artikel 82.5.

Vidare kan en personuppgiftsansvarig eller ett personuppgiftsbiträde enligt artikel 82.3 undgå skadeståndsansvar om de visar att de inte på något sätt är ansvariga för den uppkomna skadan. Vad som menas med denna formulering framgår inte av förordningen. Däremot finns i princip samma formulering i dataskyddsdirektivet, vilken det redogjorts för ovan. Enligt direktivet krävs för ansvarsfrihet force majeure eller att den registrerade bidragit till skadan. Eftersom formuleringarna är snarlika kan antas att det är detta som gäller för jämkning eller ansvarsfrihet även enligt förordningen.

När förordningen träder ikraft kommer regressrätt kunna ske på två olika sätt. Om den personuppgiftsansvarige och personuppgiftsbiträdet medverkat till samma behandling och är solidariskt skadeståndsansvariga enligt artikel 82.4, framgår regressrätten direkt av dataskyddsförordningen artikel 82.5. Eftersom culpa inte anges som krav för regressrätt enligt förordningens regel bör det finnas ett strikt ansvar för den parten som inte betalat att betala sin andel av skadan.

Om däremot den personuppgiftsansvarige eller personuppgiftsbiträdet själv ansvarar för skadan enligt artikel 82.1–82.2 kan inte regressrätt ske med stöd av förordningens artikel 82.5. Istället får då regressrätt ske med stöd av de skadeståndsrättsliga principer som nämnts ovan och då krävs culpa för att ersättning ska kunna utkrävas. Dock kan det bli svårt att vinna en regresstalan enligt art. 82.1–82.2. Om ett ansvar anses föreligga enligt dessa regler anses den andra parten inte vara inblandad i behandlingen. Att få igenom ett regresskrav kan därför vara svårt på dessa grunder.

När parterna medverkat till samma behandling kan den registrerade som sagt fritt välja att kräva betalning från antingen den personuppgiftsansvarige eller personuppgiftsbiträdet, beroende på var den registrerade har störst möjlighet att få ut full ersättning. Det företag som den registrerade väljer har ett strikt skadeståndsansvar enligt förordningen. När detta företag sedan ska regresskräva sin motpart på ersättning, kan det hända att motparten inte har möjlighet att betala. Den betalande parten kanske således inte får ersättning för hela det belopp som parten har rätt till.

Om den registrerade således vänder sig direkt till personuppgiftsbiträdet, kommer personuppgiftsbiträdet få ersätta hela den skada som den registrerade lidit genom personuppgiftsbiträdets och den personuppgiftsansvariges gemensamma behandling. Kanske kommer

[83] Hellner och Radetzki 8.u., s. 241

personuppgiftsbiträdet inte heller kunna få ersättning av den personuppgiftsansvarige för dennes del, om inte denne inte har sådana betalningsmöjligheter. Det blir således en stor skillnad för personuppgiftsbiträden, som tidigare endast kunde bli ansvariga på grund av regressrätt och då endast om de själva varit oaktsamma. Nu kan de bli direkt ansvariga, och i värsta fall även få stå för den personuppgiftsansvariges del.

Precis som i fallet med sanktionsavgifterna är en intressant fråga om ansvaret på något sätt kan fördelas genom avtal, det vill säga att den ena partens skadeståndsansvar kan begränsas på något sätt. Denna fråga har diskuterats i samma artikel som nämnts ovan i avsnittet om ansvarsfördelning av sanktionsavgifter. När den personuppgiftsansvarige och ett personuppgiftsbiträde har ett gemensamt skadeståndsansvar för en gemensam behandling enligt artikel 82.4 har den ena parten som sagt enligt förordningen artikel 82.5 ett fullständigt regresskrav gentemot den andra parten angående den partens del av skadan. Eftersom förordningens regel om regressrätt är tvingande bör den inte kunna begränsas genom avtal.

När den personuppgiftsansvarige eller personuppgiftsbiträdet själva ansvarar för skadan enligt artikel 82.1–82.2 skulle en ansvarsbegränsning genom avtal kunna vara möjlig. Om exempelvis en personuppgiftsansvarig bedöms vara orsaken till en skada, skulle den personuppgiftsansvarige kunna åberopa en ansvarsbegränsning som finns i avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Dock skulle enligt den ovan nämnda tidskriftsartikeln en domstol behöva komma fram till att biträdet bar något ansvar över huvud taget, för att skadeståndsskyldigheten skulle kunna övergå från den personuppgiftsansvarige till biträdet. Detta kan bli svårt eftersom den personuppgiftsansvarige redan bedömts som ensamt skyldig. Artikelns slutsats blir därför att skadeståndsskyldigheten i praktiken inte kommer kunna begränsas genom avtal.[84]

Detta resonemang grundar sig dock på att personuppgiftsbiträdet på något sätt måste varit oaktsamt för att skadeståndsskyldighet enligt avtal ska kunna ådömas. Som nämnts i kapitel 4.3 råder det olika åsikter om detta förhållande. Om det är som vissa jurister menar, att två parter kan avtala om ett strikt skadeståndsansvar, bör en ansvarsbegränsning genom avtal kunna bli aktuell.

[84] Frydlinger, David, *Ansvarsbegränsningar i biträdesavtal – relevanta eller irrelevanta under General Data Protection Regulation (GDPR)?* Lov&Data, nr. 128, häfte 4/2016, s. 33

6. Dataskyddsförordningens konsekvenser för personuppgiftsbiträden

6.1 Inledning

Som framställningen ovan visat kommer personuppgiftsbiträdet få nya skyldigheter och ett nytt ansvar när förordningen träder i kraft. Detta kapitel analyserar vilka positiva och negativa konsekvenser de nya reglerna kan komma att få för personuppgiftsbiträden.

6.2 Positiva konsekvenser till följd av dataskyddsförordningen

6.2.1 Skapar nya affärsmöjligheter

En positiv konsekvens till följd av dataskyddsförordningen är att förordningen skapar nya affärsmöjligheter. Företag kan nämligen använda förordningen som en affärsidé, vilket redan har börjat ske ute på marknaden. Ett exempel på en sådan affärsidé är systemet DPOrganizer. Systemet hjälper företag att föra register över sin personuppgiftsbehandling. Företagen ska på så sätt få koll på kontaktuppgifter till personuppgiftsansvariga eller personuppgiftsbiträden, vilken behandling av personuppgifter som utförs, i vilka länder behandlingen sker, osv. Systemet kan användas av både personuppgiftsansvariga och personuppgiftsbiträden. Förordningen öppnar således upp för system som kan användas som ett verktyg för att uppfylla förordningens krav på organisation av personuppgiftsbehandlingen.[85] Ett företag som tillhandahåller ett sådant system blir ett personuppgiftsbiträde åt kunden, vilket innebär att förordningen bidrar till positiva affärsmöjligheter för personuppgiftsbiträden.

En annan affärsmöjlighet som förordningen öppnar upp för är system som har ett inbyggt dataskydd och dataskydd som standard, s.k. ”Privacy by design” och ”Privacy by default”. Med detta menas att frågor om den personliga integriteten hela tiden har påverkat systemets utveckling och systemet ska därför reglera t.ex. tiden för lagring så att uppgifterna inte behandlas längre än nödvändigt.[86] Förordningen ställer i artikel 25 som krav att den personuppgiftsansvarige tar hänsyn till detta vid avgörandet om vad som är en lämplig säkerhetsåtgärd. Eftersom den personuppgiftsansvarige har en skyldighet att endast anlita de biträden som kan uppfylla de säkerhetsåtgärder som krävs, bör personuppgiftsbiträdet ta detta i beaktning vid utformandet av sina tjänster.

[85] Läs mer på www.dporganizer.com
[86] Datainspektionens faktablad, *inbyggd integritet*, januari 2012

6.2.2 Starkare skydd för personuppgifter

En annan positiv effekt, som också är syftet med förordningen, är att skyddet för personuppgifter kommer stärkas och bli mer harmoniserat i alla medlemsstater. Eftersom förordningen är överordnad nationell lag är det ett regelverk som alla EU:s medlemsstater måste följa. Observera att förordningen lämnar vissa områden oreglerade för medlemsstaterna att bestämma över själva. Ett exempel på detta är vilka sanktioner som medlemsstaterna vill använda sig av, förutom sanktionsavgifter och skadestånd. Skyddet av personuppgifter kommer därför antagligen inte vara helt harmoniserat i unionen, men det kommer förhoppningsvis bli mer harmoniserat än innan.

Vad berör molntjänster anser den Europeiska Kommissionen att de skillnader som idag finns mellan medlemsstaternas rättsliga regleringar är ett hinder för den fria användningen av molntjänster inom unionen. Det råder nämligen en oro och osäkerhet bland kunder och leverantörer angående vilket lands lagstiftning som kommer att tillämpas angående dataskydd när tjänsten sträcker sig över flera jurisdiktioner.[87] Den ökade harmoniseringen innebär alltså att ett bristande personuppgiftsskydd inte längre kommer vara ett lika stort hinder för det fria flödet av tjänster och personuppgifter på den inre marknaden. Att de nya regler som införs ger ett starkt personuppgiftsskydd innebär även att skyddet ökar i hela unionen. De betungande sanktionerna kommer förhoppningsvis även leda till att reglerna efterlevs i större omfattning än vad de gör idag.

6.3 Negativa konsekvenser till följd av dataskyddsförordningen

6.3.1 Ökad gränsdragningsproblematik mellan ansvarig och biträde

Det första problemet som de nya reglerna kan bidra till är ett större gränsdragningsproblem mellan en personuppgiftsansvarig och ett personuppgiftsbiträde. I kap 2.5 har redogjorts för den gränsdragningsproblematik som föreligger idag, nämligen att det ibland kan vara svårt att avgöra vem som bestämmer ändamål med och medel för behandlingen. Förordningen innebär ett annat sorts gränsdragningsproblem, nämligen att en personuppgiftsansvarig och personuppgiftsbiträdet i förordningen ofta behandlas på väldigt likartade sätt.

En av de nya regler som bidrar till en ökad gränsdragningsproblematik är dataskyddsförordningen art. 28.3 h) 2st., som innebär att personuppgiftsbiträdet har en skyldighet att informera den personuppgiftsansvarige om biträdet anser att den personuppgiftsansvariges

[87] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – Att frigöra de molnbaserade datortjänsternas potential i Europa, COM(2012) 529 final, s.6

instruktioner strider mot förordningen. Beroende på hur denna artikel tolkas kan detta innebära att personuppgiftsbiträdet har ett ansvar att kontrollera att den personuppgiftsansvariges instruktioner är lagenliga. Eftersom instruktionerna som den personuppgiftsansvarige lämnar bland annat ska innehålla information om ändamålen med behandlingen (se kap. 3.2.3) kan denna skyldighet innebära att biträdet ska kontrollera om behandlingens ändamål är lagenliga.

Att biträdet ska börja kontrollera behandlingens ändamål på detta sätt kan ifrågasätta rollfördelningen, särskilt eftersom det som tydligt avskiljer en personuppgiftsansvarig från ett biträde är att den ansvarige bestämmer ändamålen med behandlingen. Bestämmandet över de medel som används vid behandlingen är ofta en teknisk fråga och kan, som beskrivits i kap 2.5, ofta delegeras till personuppgiftsbiträdet. Om medlen delegeras och ändamålen kontrolleras, vem har då egentligen störst ansvar vad gäller behandlingen?

Ett annat gränsdragningsproblem gäller ansvarsfördelningen för skadestånd. Förordningen gör i denna del ingen skillnad mellan en ansvarig och ett biträde. Tvärt om kan personuppgiftsbiträdet få betala även den personuppgiftsansvariges del om denne saknar betalningsmöjligheter, eftersom skadeståndsansvaret är solidariskt vid gemensam behandling. Om personuppgiftsbiträdets roll idag till störst del är att fungera just som en leverantör av en tjänst, innebär förordningens ansvarsfördelning att biträdet ibland kommer behöva inta rollen som personuppgiftsansvarig. När en sådan situation är för handen spelar det ingen roll att biträdet egentligen har mindre skyldigheter. När en överträdelse av en gemensam skyldighet redan skett finns det inte längre någon skillnad mellan en personuppgiftsansvarig och ett personuppgiftsbiträde. Inte heller gör förordningen någon skillnad mellan en personuppgiftsansvarig och ett personuppgiftsbiträde vad gäller tillsynsmyndighetens befogenheter att utfärda sanktioner. Även här behandlas den personuppgiftsansvariga och biträdet på samma sätt.

Att personuppgiftsbiträden får ett strikt skadeståndsansvar samt kan påföras administrativa sanktionsavgifter innebär att personuppgiftsbiträden vid tillhandahållandet av sina tjänster kommer ta på sig en betydligt större ekonomisk risk än vad de gör idag. Att det blir mer riskfyllt att vara ett personuppgiftsbiträde kan komma att få konsekvenser för marknaden av IT-tjänster. En konsekvens av detta kan bli att mindre företag inte anser att det är värt risken och således slutar tillhandahålla IT-tjänster. En annan konsekvens som kan uppstå är att personuppgiftsbiträden höjer sina priser, eftersom de vill väga upp den risk de tar vid tillhandahållandet av tjänsten. Om det blir dyrare att använda sig av personuppgiftsbiträden kan en konsekvens bli att personuppgiftsansvariga hellre sköter sin IT-verksamhet

internt istället för externt. Efterfrågan på personuppgiftsbiträdens tjänster kan således komma att minska.

6.3.2 Negativa ekonomiska konsekvenser

De nya skyldigheterna och den nya ansvarsfördelningen kan innebära ekonomiska förändringar för personuppgiftsbiträdet samt påverka priset på biträdets tjänster. Dels kan det kosta en del att köpa in eller bygga upp system och andra tjänster som uppfyller de tekniska krav som förordningen ställer, framför allt med tanke på Privacy by design och Privacy by default. De personuppgiftsbiträden som inte har möjlighet att leverera ett system som uppfyller dessa krav kan därmed komma att konkurreras bort på marknaden. Det kommer ta tid, och därmed kosta pengar, för personuppgiftsbiträdet att ändra om sina rutiner så att biträdet uppfyller de skyldigheter som förordningen kräver. Anställda hos personuppgiftsbiträdet måste bland annat arbeta fram nya biträdesavtal som ska ingås med biträdets underleverantörer. Biträdet måste även kartlägga sin behandling och skapa ett sådant register som beskrivs i kap 3.3.3. Detta arbete kan vara omfattande och kräva mycket arbetskraft, vilket också är en kostnad för personuppgiftsbiträdet.

De nya skyldigheternas kostnader kan precis som den nya ansvarsfördelningen komma att påverka vilka priser som personuppgiftsbiträdena tar för sina tjänster. Om det blir dyrare och att vara ett personuppgiftsbiträde är det en naturlig konsekvens att leverantörerna kommer vilja ta mer betalt. Att personuppgiftsbiträdenas tjänster blir dyrare kan som sagt komma att påverka marknaden för sådana tjänster.

6.3.3 Särskilda konsekvenser för molntjänster

Förutom gränsdragningsproblematiken och de ekonomiska konsekvenser som beskrivits ovan, vilka påverkar samtliga personuppgiftsbiträden, förstärker dataskyddsförordningen ett särskilt problem vad gäller molntjänster och därmed för de personuppgiftsbiträden som är molntjänstleverantörer. Innan detta problem diskuteras bör nämnas att den europeiska kommissionen är positiv till användandet och utvecklingen av molntjänster, vilket de uttryckte i ett meddelande till Europaparlamentet m.fl. år 2012.[88] Enligt detta meddelande vill kommissionen satsa på utvecklingen av molntjänster och har en förhoppning om att Europa ska säkra en ledarplats i denna utveckling. Kommissionen understryker även alla fördelar som molntjänster innebär.

[88] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – Att frigöra de molnbaserade datortjänsternas potential i Europa, COM(2012) 529 final

Bland dessa fördelar kan nämnas att kunden kan använda sin mjukvara när och var det än behövs, att kunden bara behöver betala för själva nyttjandet av tjänsten och således slipper slösa resurser, att kunden inte behöver göra några kapitalinvesteringar i form av hårdvara, m.m. Kommissionen redovisar även resultat från en rapport som utfördes åt kommissionen år 2011. Av denna rapport framgår att utnyttjandet av molntjänster kan minska en organisations kostnader med 10–20 % i 80 % av fallen. Vidare redovisas att molntjänster bland annat kan öka organisationers produktivitet med 41 % och organisationers affärsmöjligheter med 33 %. Sammanfattningsvis kan således sägas att molntjänster har många fördelar.

Kommissionen menar att ett av de problem som hindrar utvecklingen av molntjänster är den bristande harmonisering som råder angående dataskydd inom unionen. Detta var en av anledningarna till att kommissionen lade fram förslaget till dataskyddsförordningen år 2012. För att få en harmoniserad dataskyddslagstiftning inom medlemsstaterna och därmed undanröja ett hinder för utvecklingen av molntjänster.

Dataskyddsförordningen kan dock innebära problem för molntjänster. I dataskyddsförordningen artikel 30 anges att den personuppgiftsansvarige ska upprätta ett register över personuppgiftsbehandlingen. I samma artikel i punkten 1 e) anges att den personuppgiftsansvarige i registret ska ange om överföringar av personuppgifter kommer ske till ett tredje land och i så fall vilket land. Denna reglering finns till för att den registrerade, enligt dataskyddsförordningen artikel 13 och 14, har rätt att få information från den personuppgiftsansvarige angående behandlingen av sina personuppgifter, inbegripet om personuppgifterna överförs till tredje land.

Problemet med detta är att kravet kolliderar med molntjänstens tredje och väsentliga karaktärsdrag, nämligen det som kallas för ”Resource pooling”. Som beskrivits i kap 2.2. innebär Resource pooling att en tjänst, för att utgöra en molntjänst, ska uppfattas som ett system av kunden. Kunden ska inte behöva veta var leverantörens servrar är placerade, hur tjänsten är uppbyggd tekniskt m.m.

När den personuppgiftsansvarige genom förordningen får en skyldighet att informera den registrerade om var hans eller hennes personuppgifter befinner sig, och därigenom skapa det ovan beskrivna registret över personuppgiftsbehandlingen, uppstår ett problem. Den personuppgiftsansvarige måste på grund av denna skyldighet veta var den anlitade molntjänstleverantören lagrar personuppgifterna. Den personuppgiftsansvarige behöver således veta var molntjänstleverantören har sina servrar, för den händelse att servern befinner sig i ett tredje land. Ett av molntjänsternas viktiga karaktärsdrag kolliderar alltså med dataskyddsförordningen.

Observera att detta problem finns även idag. Dataskyddsdirektivet artikel 25 och 33 § personuppgiftslagen uppställer ett förbud mot att personuppgifter överförs till ett tredje land som inte har en adekvat skyddsnivå. Indirekt innebär detta att den personuppgiftsansvarige har en skyldighet att veta var personuppgifterna behandlas. Datainspektionen har bekräftat att personuppgiftsansvariga har en sådan skyldighet i ett tillsynsärende som rörde en kommuns användning av molntjänsten Microsoft Office 365.

Vid Datainspektionens granskning av kommunens användning av molntjänsten fann Datainspektionen att användningen inte uppfyllde de krav som dataskyddsdirektivet och personuppgiftslagen uppställer angående personuppgiftsbehandlingen. Anledningen var att Microsofts uppräkning av underleverantörer på sin hemsida inte angav underleverantörernas lokalisering, utan endast firmanamnet och vilken typ av uppdrag som utfördes av underleverantören.[89] Datainspektionen kräver således även idag att den personuppgiftsansvariga vet i vilket land all personuppgiftsbehandling sker.

Dataskyddsförordningen gör dock detta krav tydligare, och uppställer som sagt betungande sanktioner om förordningen inte efterlevs. Även om det tidigare funnits en kollision mellan ett av molntjänsternas karaktärsdrag och personuppgiftsskyddet kommer denna kollision bli mer aktuell än tidigare. Det återstår att se vilken effekt detta kommer att ha på molntjänster.

[89] DI 1475-2013 (2014-04-25)

7. Avslutande kommentar

Precis som rubriken till denna uppsats indikerar kommer personuppgiftsbiträdens roll förändras när dataskyddsförordningen träder ikraft 2018. Om ett personuppgiftsbiträde tidigare varit ett osjälvständigt hjälpmedel till den personuppgiftsansvarigas behandling av personuppgifter, kommer personuppgiftsbiträdet nu upphöjas till samma ansvarsnivå som den personuppgiftsansvariga. Det blir intressant att se vilka effekter detta kommer få, framförallt på marknaden för IT-tjänster.

Förutom det nya ansvaret och de betungande sanktioner som personuppgiftsbiträdet kan påföras, innebär de många nya skyldigheter som förordningen kräver praktiska svårigheter. Det kan ifrågasättas om de krav som förordningen ställer ens kommer vara möjliga att uppfylla i verkligheten. Är det exempelvis praktiskt möjligt att lokalisera samtliga av en människas personuppgifter i alla de olika system ett företag kan ha personuppgifter i? Är det möjligt att radera även de personuppgifter som hamnat i en backup?

En annan intressant fråga är hur Datainspektionen kommer att använda sina nya befogenheter. Kommer Datainspektionen utdela administrativa sanktionsavgifter på det sätt som förordningen ger möjlighet till, eller kommer myndigheten utnyttja undantaget ”mindre överträdelser” och därmed utdela reprimander istället för att utdela de kraftiga administrativa sanktionsavgifterna? Även EU-domstolen kommer med största sannolikhet att få fullt upp när alla EU:s medlemsstater vill ha en tolkning av de begrepp som lämnats oförklarade, t.ex. ”mindre överträdelser” eller ”utan onödigt dröjsmål”.

Hur det än går står klart att detta nya regelverk kommer ha inverkan både på ett juridiskt plan och i näringslivet. Det kommer bli väldigt intressant att iaktta den utveckling som kommer följa efter förordningens ikraftträdande, den 25 maj 2018.

8. Källförteckning

8.1 Litteratur

Bengtsson, Bertil, *Allmänna principer om kontraktansvar*, Lindell-Frantz Eva (Red.), Festskrift till Lars Gorton, Juristförlaget, Lund, 2007

Christner, Anders och Edvardsson, Tobias, *Cloud Computing – en handledning och kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010*, 2011 (förlag och förlagsort okänt)

Frydlinger, David, *Ansvarsbegränsningar i biträdesavtal – relevanta eller irrelevanta under General Data Protection Regulation (GDPR)?* Lov&Data, nr. 128, häfte 4/2016

Hellner, Jan och Radetzki, Marcus, *Skadeståndsrätt*, 9:1 u., Nordstedts Juridik AB, Stockholm, 2014

Hellner, Jan och Radetzki, Marcus, *Skadeståndsrätt*, 8:2 u., Nordstedts Juridik AB, Stockholm, 2012

Korling, Fredric och Zamboni, Mauro (Red.), *Juridisk metodlära*, 1.5 u., Studentlitteratur AB, Lund, 2015

Magnusson Sjöberg, Cecilia (red.), *Rättsinformatik – Juridiken i det digitala informationssamhället*, 2 u., Studentlitteratur AB, Lund, 2016

Mell, Peter och Grance, Timothy, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, September 2011

Perméus, Anders och Lindberg, Daniel, IT-avtal – *En kommentar till IT-branschens standardavtal*, Jure Förlag AB, Stockholm, 2013

Ramberg, Jan & Ramberg, Christina, *Allmän avtalsrätt*, 10 u., Wolters Kluwer Sverige AB, Stockholm, 2016, s. 238

Sjöberg, Personuppgiftslag (1998:204) 3 §, Lexino 2015-12-31 (Lagkommentar)

Öman, Sören och Lindblom, Hans-Olof, *Personuppgiftslagen - En kommentar*, 4:2 u., Stockholm, Nordsteds Juridik AB, 2011

8.2 Offentligt tryck

Prop. 2003/04:121 Ny produktsäkerhetslag

Prop. 2001/02:144 Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten

Prop. 1997/98:44 Personuppgiftslag

Prop. 1981/82:142 ändring i brottsbalken (ekonomiska sanktioner vid brott i näringsverksamhet)

SOU 2016:58 Ändrade mediegrundlagar

SOU 2015:39 Myndighetsdatalag

SOU 1997:39 Integritet, offentlighet, informationsteknik

Datainspektionens vägledande dokument, *Vad är straffbart enligt personuppgiftslagen? – En vägledning från Datainspektionen för polis och åklagare*, januari 2011

Datainspektionens allmänna råd, *Säkerhet för personuppgifter*, Stockholm, reviderad version november 2008

Datainspektionens faktablad, *Inbyggd integritet*, januari 2012

8.3 Rättsfall

NJA 2013 s. 1046

8.4 Svensk publicerad myndighetspraxis

DI 1475-2013 (2014-04-25)

8.5 Författningar

Bokföringslag (1999:1078)

Konkurrenslag (1993:20)

Marknadsföringslag (1995:450)

Personuppgiftslag (1998:204)

Produktsäkerhetslag (2004:451)

Skadeståndslag (1972:207)

8.6 Internetkällor

http://www.ne.se/ezp.sub.su.se
Nationalencyklopedin, backup (hämtad 2016-12-14)

http://www.ne.se.ezp.sub.su.se
Nationalencyklopedin, server (hämtad 2016-12-13)

www.dporganizer.com

8.7 Europarättsligt material

8.2.1 Europeiska unionens rättsakter

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

Europaparlamentet och Rådets Förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 94/46 EG

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

Europaparlamentets och rådets direktiv 2001/95 EG av den 3 december 2011 om allmän produktsäkerhet

8.2.2 EU-domstolens praxis

Mål C-322/88, Grimaldi mot Fonds des maladies professionnelles, ECLI:EU:C:1989:646

8.2.3 Soft law

Europeiska Kommissionens förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning) COM (2012) 11 final

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – Att frigöra de molnbaserade datortjänsternas potential i Europa, (COM(2012) 529 final

Europaparlamentets meddelande till ledamöterna nr. 8/2004 Förslag till betänkande med rekommendationer till Kommissionen om ett vägledande europeiskt tabellverk över skadors inverkan på den fysiska och mentala integriteten (2003:2130(INI))

Artikel 29-arbetsgruppens yttrande 05/2014 om avidentifieringsmetoder antaget den 10 april 2014

Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing) antaget den 1 juli 2012

Artikel 29-arbetsgruppens yttrande 1/2010 om begreppen registeransvarig och registerförare, antaget den 16 februari 2010

Artikel 29-arbetsgruppens yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society for Worldwide Interbank Financial Telecommunication) antaget den 22 november 2006