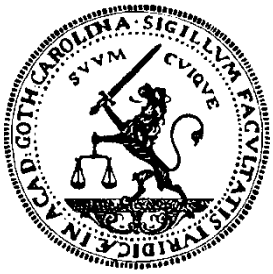

JURIDISKA FAKULTETEN

vid Lunds universitet

Gustav Wahlberg

GDPR:s påverkan på due diligence-processen vid ett företagsförvärv

LAGM01 Examensarbete

Examensarbete på juristprogrammet

30 högskolepoäng

Handledare: Katarina Olsson

Termin för examen: period 1 VT2019

Innehållsförteckning

Summary **4**

Sammanfattning **5**

Förkortningar **6**

Förord **7**

1. Inledning **1**

1.1 Bakgrund **1**

1.2 Syfte **2**

1.3 Metod och Material **2**

1.4 Avgränsningar **4**

1.5 Disposition **5**

2. Due diligence **7**

2.1 Inledning **7**

2.2 Rättslig reglering av due diligence **7**

2.3 Informationshantering vid due diligence **9**

2.4 Aktörerna i en due diligence **11**

3. GDPR **12**

3.1 Inledning **12**

3.2 Tillämpningsområde **13**

3.2.1 Materiellt tillämpningsområde 13

3.2.2 Territoriellt tillämpningsområde 14

3.3 Grundläggande begrepp **15**

3.3.1 Personuppgifter 15

3.3.2 Personuppgiftsbehandling 16

3.3.3 Personuppgiftsansvarig 18

3.3.4 Personuppgiftsbiträde 20

3.3.5 Personuppgiftsansvariges och personuppgiftsbiträdets ansvar 21

3.4 Behandling av personuppgifter **22**

3.4.1 Inledning 22

3.4.2 Laglig personuppgiftsbehandling 22

3.4.2.1 Samtycke som rättslig grund ... 22
3.4.2.2 Nödvändighet som rättslig grund ... 24
3.4.3 De registrerades rättigheter ... 26
3.4.3.1 Säkerhet i samband med behandlingen ... 26
3.4.3.2 Överföring av personuppgifter till andra personuppgiftsansvariga ... 28
3.4.3.3 Informationskraven i artikel 13 och 14 ... 30
4. Due diligence och GDPR ... 32
4.1 Inledning ... 32
4.2 Rättslig grund ... 32
4.2.1 Rättslig grund för att lägga in personuppgifter i datarum ... 32
4.2.2 Handlingsförslag för säkerställande av regelefterlevnad ... 35
4.3 Säkerhetsåtgärder ... 37
4.3.1 Säkerhetsåtgärder och due diligence ... 37
4.3.2 Handlingsförslag för säkerställande av regelefterlevnad ... 38
4.4 Överföring till annan personuppgiftsansvarig ... 40
4.4.1 Överföring inom EU ... 40
4.4.2 Överföring utanför EU ... 40
4.4.3 Handlingsförslag för säkerställande av regelefterlevnad ... 42
4.5 Informationskraven i artikel 13 och 14 GDPR ... 43
4.5.1 Informationskraven vid en due diligence ... 43
4.5.2 Handlingsförslag för säkerställande regelefterlevnad ... 45
5. Sammanfattande slutsatser ... 49
5.1 Informationshanteringen vid en due diligence omfattas av GDPR ... 49
5.2 Rättslig grund för hantering av personuppgifter vid en due diligence ... 49
5.3 Vidtagande av säkerhetsåtgärder i samband med en due diligence ... 50
5.4 Överföring av personuppgifter till annan personuppgiftsansvarig ... 50
5.5 Uppfyllande av informationskravet i samband med en due diligence ... 51
5.6 Generella slutsatser ... 51
Käll- och litteraturförteckning ... 52
Rättsfallsförteckning ... 58

Summary

The commencement of the new data protection regulation, GDPR, entails increased requirements on companies when it comes to their processing of personal data. The due diligence that is carried out in connection with an M&A does in most cases contain some kind of processing of personal data. This induces the purpose of this essay, which is to investigate whether the information-management associated with a due diligence is affected by the rules in GDPR.

The information-management in connection with a due diligence implies processing of personal data according to GDPR and therefore a lawful basis is required in order to process personal data in a due diligence. It is not possible to determine a lawful basis for processing of personal data in a due diligence. However, the balancing-of-interest in article 6.1 f GDPR seems to be applicable depending on the circumstances of each case. In order to increase the probability for a balancing-of-interest to result in lawful basis there is some actions for the controller to take. Such actions could for example be limitation of the amount of processed personal data, pseudonymisation and anonymisation of personal data. Actions of the above kind and actions as separate dataroom for the HR-department and detailed confidentiality agreements could further be required to fulfil the requirements in GDPR as for taking appropriate technical and organisational measures.

Furthermore, a due diligence could contain a transfer of personal data from the controller to another controller. If the transfer is within the EU the conventional rules for processing of personal data applies. However, if the transfer is made to a receiver in a third country special rules apply. In order for a third country-transfer to be in compliance with GDPR it has to fulfil any of the terms that is stated in chapter five of the regulation. Article 46 GDPR prescribes, among other things, that a transfer to a third country is lawful if the transferring part and the receiver enter into an agreement which contains standard clauses adopted by the Commission or clauses formed by the parties after authorisation by Datainspektionen. The above-mentioned term is the term that appears to be applicable for a transfer in connection with a due diligence. Additionally, GDPR requires the controller to inform the data subjects when a transfer of personal data occurs. Although, there are some exceptions to the requirement of information which could be fulfilled by a precept in the privacy policy of the controller.

Accordingly it could be stated that GDPR affects the information-management in a due diligence. The impact primarily appears with regard to the measures the involved parties have to take in order to be in compliance with GDPR. Because of the fact that many of the provisions in GDPR are dependent on the circumstances of each case it has however, to some extent, been hard to draw concrete conclusions.

Sammanfattning

Ikraftträdandet av den nya dataskyddsförordningen, GDPR, medför ökade krav på företag när det kommer till företagens behandling av personuppgifter. Den due diligence som genomförs i samband med ett företagsförvärv innefattar i de allra flesta fall någon form av personuppgiftsbehandling. Vilket föranleder uppsatsens syfte som är att utreda huruvida informationshanteringen vid en due diligence påverkas av reglerna i GDPR.

Informationshanteringen vid en due diligence innebär en personuppgiftsbehandling enligt GDPR och således krävs det rättslig grund för att behandla personuppgifter i samband med en due diligence. Det är inte möjligt att fastställa en rättslig grund för personuppgiftsbehandling i samband med en due diligence. Däremot förefaller intresseavvägningen i artikel 6.1 f GDPR vara tillämplig beroende på omständigheterna i varje enskilt fall. I syfte att öka sannolikheten för att en intresseavvägning leder till rättslig grund finns det åtgärder som den personuppgiftsansvarige kan vidta. Sådana åtgärder kan till exempel vara begränsning av antalet behandlade personuppgifter, pseudonymisering och anonymisering av personuppgifter. Åtgärder av ovan nämnda slag och åtgärder som till exempel ett separat datarum för HR-avdelningen och utförliga sekretessavtal kan dessutom krävas för att tillgodose kraven i GDPR vad gäller vidtagande av lämpliga tekniska och organisatoriska åtgärder.

Vidare kan det vid en due diligence bli aktuellt för den personuppgiftsansvarige att överföra personuppgifter till en annan personuppgiftsansvarig. Vid en överföring inom EU gäller de sedvanliga reglerna för personuppgiftsbehandling. I det fall att överföringen sker till en mottagare i ett tredjeland gäller istället särskilda regler. För att en överföring utanför EU ska vara förenlig med GDPR krävs att något av villkoren i förordningens kapitel fem är uppfyllt. Artikel 46 GDPR föreskriver bland annat att överföringen är lagenlig om den överförande parten och mottagaren ingår avtal som innehåller standardavtalsklausuler accepterade av EU-kommissionen alternativt egen utformade avtalsklausuler efter godkännande av Datainspektionen. Ovanstående villkor är det villkor som förefaller vara tillämpligt vid en överföring i samband med en due diligence. GDPR medför dessutom krav på att den personuppgiftsansvarige ska informera de registrerade vid en överföring av personuppgifter till annan personuppgiftsansvarig. Det finns dock undantag från informationskravet vilket skulle kunna uppfyllas genom en skrivelse i den personuppgiftsansvariges personuppgiftspolicy.

Följaktligen kan det konstateras att GDPR påverkar informationshanteringen vid en due diligence. Påverkan ger sig först och främst till känna genom att aktörerna i en due diligence behöver vidta olika åtgärder för att reglerna i GDPR ska efterlevas. På grund av att många av bestämmelserna i GDPR är beroende av omständigheterna i varje enskilt fall har det dock, i viss mån, varit svårt att dra konkreta slutsatser.

Förkortningar

AI	Artificiell Intelligens
AvtL	Lag om avtal och andra rättshandlingar på förmögenhetsrättens område (1915:218)
Dataskyddsdirektivet	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
Dataskyddslagen	Lag med kompletterande bestämmelser till EU:s dataskyddsförordning(2018:218)
EDPB	Europeiska Dataskyddsstyrelsen
GDPR	Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27april 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 95/46/EG (allmän dataskyddsförordning)
KöpL	Köplag(1990:931)
PUL	Personuppgiftslag(1998:204)

Förord

Nu när det är dags att lämna in examensarbetet och avsluta mina 4 år i Lund skulle jag vilja passa på att tacka min handledare Katarina Olsson för mycket bra handledning genom bra synpunkter och råd. Dessutom skulle jag vilja rikta ett stort tack till min familj för bra stöd genom hela utbildningen. Sedan skulle jag, trots minimalt stöd, vilja tacka mina vänner för fyra härliga år i Lund. Slutligen vill jag tacka IFK Göteborg för att ni har förgyllt våren med er vansinnigt fina fotboll.

Gustav Wahlberg, 23/5 2019 Lund.

1. Inledning

1.1 Bakgrund

Den 25 maj 2018 trädde den nya dataskyddsförordningen, GDPR, i kraft.[1] Syftet med införandet av GDPR är att skydda enskildas rättigheter och friheter, i synnerhet deras rätt till skydd för personuppgifter. Vidare syftar GDPR till att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU.[2] GDPR medför ökade krav på företag vad gäller deras hantering av personuppgifter och den som inte följer dessa regler riskerar höga sanktionsavgifter.[3] Förutom den föreliggande risken för höga sanktionsavgifter är regelefterlevnad av GDPR dessutom en trovärdighetsfråga som påverkar ett företags varumärke, företag som missbrukar personuppgifter riskerar att tappa i trovärdigheten och relevansen gentemot kunderna.[4]

Den svenska marknaden för företagsförvärv har under se senaste åren haft en stabil tillväxt, dessutom fortsätter marknaden att växa.[5] Vidare har komplexiteten av företagsförvärven ökat, bland annat på grund av att antalet utländska aktörer på den svenska företagsförvärvsmarknaden blir fler och fler.[6] Med hänsyn till den stigande komplexiteten har vikten av en grundligt utförd due diligence ökat. En väsentlig del av due diligence-arbetet består i hantering av olika typer av information. Information i form av personuppgifter är vanligt förekommande vid informationshanteringen i en due diligence.

Frågan är därför hur reglerna i GDPR kommer att påverka due diligence-arbetet och därigenom vilka åtgärder aktörerna i ett due diligence-förfarande måste vidta för att säkerställa att GDPR efterlevs.

---

[1] Art 99. GDPR.
[2] Datainspektionen, *Dataskyddsförordningen syfte och tillämpningsområde*.
[3] Art 83. GDPR.
[4] Bolter(2019).
[5] Bolander (2019).
[6] Höiseth(2019).

1.2 Syfte

Syftet med uppsatsen är att utreda huruvida informationshanteringen vid den due diligence som företas i samband med ett företagsförvärv påverkas av reglerna i GDPR. Således ämnar uppsatsen utreda vilka delar av informationshanteringen som eventuellt påverkas av reglerna i GDPR samt vad en potentiell påverkan kan medföra för effekter och frågeställningar i due diligence-arbetet. Dessutom syftar uppsatsen till att undersöka hur förekommande effekter och frågeställningar kan hanteras inom ramen för en due diligence.

1.3 Metod och Material

Syftet med uppsatsen uppnås med hjälp av en rättsdogmatisk metod. Den rättsdogmatiska metoden utgår från principerna för användandet av de allmänt accepterade rättskällorna vilket innebär att lagstiftning, förarbeten, rättspraxis och doktrin studeras för att utröna vad som är gällande rätt.[7] Med hänsyn till att det finns ett relativt stort antal allmänt accepterade rättskällor avseende företagsförvärv, due diligence och GDPR lämpar sig den rättsdogmatiska metoden väl.

Det finns ingen lag som uttryckligen reglerar företagsförvärv och due diligence. Däremot kan köplagen(1990:931), KöpL, tillämpas på ett företagsförvärv varför KöpL, dess förarbeten samt praxis och doktrin tillhörande KöpL används vid utredningen av due diligence. Reglerna i KöpL används således för att utröna vad som är gällande rätt när det kommer till due diligence och därigenom för att uppnå uppsatsens syfte avseende informationshanteringen vid en due diligence. Propositionen till den nya KöpL används för att förtydliga den rättsliga bakgrunden till en due diligence.[8] Praxis på området är relativt begränsad. En anledning till den begränsade mängden praxis är att de flesta tvisterna på området avgörs genom skiljeförfarande vilket medför att de avgöranden som finns sällan blir offentliga. Praxis används ändå i viss utsträckning för att dra slutsatsen att KöpL är tillämplig på företagsförvärv.[9] NJA 1976 s. 341 hänför sig dock till den äldre KöpL vilket medför anledning att vara försiktig med vilka slutsatser som dras utifrån rättsfallet. Det som används från rättsfallet är dock allmänna principer vilket torde innebära att slutsatserna är tillämpliga

[7] Nääv och Zamboni(2018) s. 21.
[8] Prop 1988/89:76 *om ny köplag*.
[9] NJA 1976 s. 341.

även på den nya KöpL. Vad gäller doktrin avseende due diligence föreligger det brist på mer djupgående redogörelser. Däremot finns Christina Rambergs avhandling, *kontraktsbrott vid köp av aktie,* som behandlar aktieöverlåtelser och vilka obligationsrättsliga problem som därigenom kan uppkomma.[10] Dessutom används Forssmans bok om företagsöverlåtelser[11] samt Sevenius böcker om företagsförvärv[12] och due diligence[13].

Vid utredningen om regleringen av insamling och hantering av personuppgifter är naturligtvis GDPR central. Skälen till GDPR samt svenska förarbeten till införandet av GDPR i Sverige har en väsentlig roll för att utreda och tolka bestämmelserna i GDPR.[14] Som nämnts ovan trädde GDPR i kraft den 25 maj 2018 vilket medför att praxis och doktrin på området är relativt begränsad. Praxis från EU-domstolen som rör det tidigare gällande dataskyddsdirektivet, Direktiv 95/46/EG, kan dock användas för att tolka bestämmelserna i GDPR. Dessutom finns det yttranden och rekommendationer från EU-organet, *Artikel 29-gruppen,* som kan användas för att tolka GDPR.[15] Artikel 29-gruppen var en rådgivande och oberoende organisation som skulle se till att det tidigare gällande dataskyddsdirektivet tillämpades enhetligt i medlemsstaterna. Vid införandet av GDPR ersattes organisationen av den Europeiska dataskyddsstyrelsen, EDPB.[16] Följaktligen kan även yttranden och beslut från den här nyskapade organisationen användas, det bör dock noteras att de i nuläget inte har hunnit producera särskilt mycket material. I det här avseendet bör det även uppmärksammas att en del av artikel 29-gruppens arbete är relativt gammalt, riktlinjerna avseende personuppgiftsansvarig och personuppgiftsbiträde är exempelvis från 2010. Det nyinrättade organet håller i skrivande stund på med att ta fram nya riktlinjer för dessa begrepp.[17] Således kan begreppen, och även annat i GDPR, komma att tolkas på ett annorlunda sätt i framtiden. Vidare finns det praktisk litteratur att tillgå för att öka förståelsen för GDPR, *GDPR : - juridik, organisation och säkerhet enligt dataskyddsförordningen*[18] och *The EU General Data Protection Regulation (GDPR) - A pracital guide*[19] är två av dessa verk.

---

[10] Ramberg(1992).
[11] Forssman(2016).
[12] Sevenius(2011).
[13] Sevenius(2013).
[14] Prop 2017/18: 105 *Ny dataskyddslag* och SOU 2017:39 *Dataskyddsutredningen*.
[15] Europeiska Kommissionen, *Opinons and recommendations.*
[16] Dataisnpektionen, *Så här är dataskyddet organiserat i EU.*
[17] Datainspektionen, *Datainspektionen leder arbete med nya EU-riktlinjer.*
[18] Frydlinger m.fl.(2018).
[19] Voigt & von Dem Bussche(2017).

1.4 Avgränsningar

Vid ett företagsförvärv utförs vanligtvis flera olika typer av due diligence. Eftersom det är en juridisk uppsats kommer den av förklarliga skäl enbart fokusera på legal due diligence. Vidare kommer uppsatsen, med hänsyn till dess syfte, att inrikta sig mot personuppgifter när det kommer till utredningen om insamling och hantering av information vid en due diligence vilket medför att annan information som till exempel företagshemligheter inte kommer att behandlas.

Det bör även observeras att den rättsliga utredningen av GDPR kommer att begränsas genom att, i mångt och mycket, fokusera på bestämmelser som uppbär relevans för en due diligence. Därigenom kommer vissa delar av GDPR att utelämnas och därför är det ingen fullständig utredning av GDPR.

Med hänsyn till de höga böter som ett företag riskerar på grund av GDPR kommer det vara viktigt vid en due diligence att utreda huruvida målbolagets personuppgiftshantering är förenlig med GDPR, en så kallad GDPR-due diligence. En sådan utredning kräver besvarande av frågor som till exempel: *Har målbolaget utsett ett dataskyddsombud? Har målbolaget inhämtat personuppgifter på rättslig grund?* Uppsatsen kommer dock inte att utreda sådana spörsmål utan enbart fokusera på hur själva informationshanteringen påverkas av GDPR.

Ytterligare en begränsning av uppsatsens framställning avser utredningen om GDPR:s ansvarsregler. Innan en due diligence påbörjas brukar advokatbyråerna dels sinsemellan och dels gentemot sina uppdragsgivare och datarumsleverantör reglera eventuella ansvarsfrågor genom avtal, exempelvis genom olika former av ansvarsbegränsningar. Således hade det varit intressant att utreda hur sådana avtalsrättsliga ansvarsbestämmelser förhåller sig till reglerna om ansvar i GDPR. En sådan utredning hade dock riskerat att hamna utanför uppsatsens syfte varför en utredning av frågan har utelämnats i denna uppsats.

Teknologin för artificiell intelligens, AI, har utvecklats de senaste åren och tillämpningsområdena för teknologin blir allt fler.[20] AI har dessutom börjat användas inom juridiken, framförallt vid due diligence-processer. Dessutom tror många att användning av AI

[20] Selbts(2018).

kommer att bli allt vanligare inom juridiken.[21] AI:s inträde inom juridiken föranleder flera frågeställningar som hade varit intressanta att utreda. Däribland hur användningen av AI vid ett due diligence-förfarande förhåller sig till reglerna i GDPR, exempelvis vad gäller regler om transparens och automatiserat beslutsfattande. Den här uppsatsen kommer dock inte att beröra sådana frågeställningar annat än i ytterst begränsad omfattning. Ovanstående avgränsning beror på att användningen av AI i svenska due diligence-förfaranden fortfarande är i startgroparna samt att uppsatsen hade riskerat att bli allt för omfattande och brista i sin tydlighet vid adderande av en sådan utredning.

1.5 Disposition

I uppsatsens *andra kapitel* återfinns en redogörelse för legal due diligence. Först och främst presenteras den rättsliga regleringen av en due diligence. Kapitlet fokuserar sedan på informationshanteringen vid en due diligence, vilket inkluderar hur informationen samlas in samt görs tillgänglig för de inblandade aktörerna i en due diligence. Slutligen redogör kapitlet för vilka aktörerna i en due diligence är.

Det *tredje kapitlet* innehåller en rättslig utredning av GDPR. Utredningen är, i mångt och mycket, av allmän karaktär men för att konkretisera utredningen återges en del exempel som är relevanta för uppsatsens syfte. Inledningsvis utreds GDPR:s tillämpningsområde, dels det materiella tillämpningsområdet och dels det territoriella tillämpningsområdet. Sedan utreds ett antal begrepp som är centrala för att få en förståelse för många av bestämmelserna i GDPR. Till sist innehåller kapitlet en redogörelse för behandling av personuppgifter där rättslig grund för behandling och de registrerade personernas rättigheter har en central betydelse.

I det *fjärde kapitlet* kopplas det andra och tredje kapitlet ihop genom en utredning av hur reglerna i GDPR påverkar due diligence-processen. Kapitlet inleder med att utreda vilken rättslig grund som kan vara tillämplig vid informationshanteringen i en due diligence. Vidare presenteras vilka säkerhetsåtgärder som kan vara aktuella att vidta vid en due diligence. Dessutom innehåller kapitlet en redogörelse för reglerna om överföring av personuppgifter till annan personuppgiftsansvarig, i synnerhet vad gäller överföring till en

[21] Persson och Knutsson(2017) s.38-ff.

personuppgiftsansvarig som befinner sig utanför EU. Slutligen analyseras det informationskrav som stadgas i GDPR och hur det aktualiseras vid en due diligence-process

Det sista och *femte kapitlet* innehåller en sammanfattning av de slutsatser som uppsatsens förevarande kapitel resulterat i.

2. Due diligence

2.1 Inledning

Förvärvandet av ett företag är förknippat med stora risker och det finns ett flertal faktorer som kan leda till att ett förvärv blir misslyckat. Dessutom kan det uppstå tvister mellan köpare och säljare rörande förvärvet och därför är det essentiellt att avgöra riskfördelningen avseende felaktiga förutsättningar i rättsförhållandet mellan dessa parter.[22] Vid de allra flesta förvärv utförs därmed en due diligence, vilket är ett sätt att fördela risken mellan parterna.

Den vanligaste formen av due diligence är en så kallad köpar-due diligence. En sådan due diligence genomförs av en potentiell köpare tillsammans med dess rådgivare och innefattar en genomgång av bolaget. Säljaren ansvarar sedermera för att samla in material som köparen får tillgång till. Vilket material som görs tillgängligt baseras vanligtvis mot bakgrund av en frågelista som köparen skickar till säljarens ombud. Det huvudsakliga syftet med utförandet av en due diligence är att hitta eventuella brister och risker i målbolaget före köpet.[23] Undersökningen delas vanligtvis upp i olika kategorier som till exempel bolagsrätt, arbetsrätt, tvister, fastigheter och immaterialrätt. Beroende på storleken av ett förvärv blir olika typer av risker relevanta, om det till exempel är en stor transaktion förbises risker som kan leda till brister av ett mindre värde. En vanlig riskfaktor är en så kallad *change of control-klausul* i olika avtal, en klausul som innebär att avtalsparten har rätt att säga upp avtalet i det fall att målbolaget byter ägare. När en sådan klausul finns i ett avtal är det givetvis en risk som bör uppmärksammas.[24] Det bör även noteras att det har blivit allt mer vanligt att säljaren utför en så kallad *vendor due diligence*, vilket innebär att säljaren utför en egen due diligence innan köparen får tillgång till datarummet.[25]

2.2 Rättslig reglering av due diligence

Det finns ingen lag som uttryckligen reglerar företagsförvärv och due diligence. Som huvudregel gäller principen om avtalsfrihet med undantag för vad som gäller enligt lag och

[22] Sevenius(2013) s.46 ff.
[23] Forssman(2016) s.26.
[24] Ibid. s.43.
[25] Ibid. s.26.

avtalsrättsliga principer som exempelvis reglerna i Lag om avtal och andra rättshandlingar på förmögenhetsrättens område (1915:218), AvtL, om ogiltighet och jämkning.[26] Därmed är frågan om vilken lag som är tillämplig på ett företagsförvärv av mindre vikt i praktiken. Däremot kan det uppstå många olika situationer och det är därför svårt att reglera alla typer av situationer i ett avtal, vilket medför att frågan om tillämplig lag ändå uppbär relevans. Det har tidigare rått en viss debatt om vilken lag som ska tillämpas vid överlåtelse av hela eller delar av aktierna i ett bolag, numer får det dock anses klarlagt att KöpL är tillämplig på sådana företagsförvärv.[27] KöpL är enligt dess 3 § dispositiv vilket medför goda möjligheter att avtala bort KöpL. Enligt Sevenius krävs det dock att parterna uttryckligen avtalar bort KöpL samt preciserar vad som ska gälla istället för att möjliggöra ett åsidosättande av lagen.[28]

Det har ovan konstaterats att KöpL är tillämplig på ett företagsförvärv, och en due diligence huvudsakliga rättsliga betydelse härstammar just från att fördela den köprättsliga risken mellan köpare och säljare.[29] En köpare och säljare i ett företagsförvärv är bundna till varandra i ett obligationsrättsligt förhållande, vilket medför att den köprättsliga riskfördelningen mellan parterna är fullständig, följaktligen bär alltid någon av parterna risken för felaktigheter i rättsförhållandet.[30]

Enligt 17 § 1st KöpL gäller att köpeobjektet ska stämma överens med vad som följer av köpeavtalet, således står säljaren risken för att köpeobjektet stämmer överens med det som stadgas i köpeavtalet. Vidare gäller enligt 17 § 3st. KöpL att säljaren står risken för att köpet avviker från köparens befogade förväntningar. Med *köparens befogade förväntningar* avses de förväntningar som en normalt begåvad köpare skulle ha vid ett köp av det aktuella köpeobjektet. Det kan dock vara problematiskt att avgöra vad som är befogade förväntningar på ett målföretag med tanke på att det är ett unikt köpeobjekt och att det kan vara svårt att hitta en jämförelsenorm för vad som ska anses vara normalt för en affärsdrivande verksamhet.[31] 20 § KöpL medför dock en begränsning av säljarens risk. För det första får

[26] Ramberg(1992) s.37.
[27] Forssman(2016) s.15., Ramberg (1992) s. 85, Lindskog (1990) s. 142-f och NJA 1976 s. 341.
[28] Sevenius(2011) s.349.
[29] Sevenius(2013) s.317.
[30] Ibid. s.320.
[31] Ibid. s.322.

köparen inte åberopa sådant som hen har kännedom om.[32] Dessutom begränsas säljarens risk genom att om en köpare företagit en undersökning, alternativt underlåtit att undersöka objektet trots att säljaren uppmanat till det, inte såsom fel får åberopa sådant som hen upptäckt eller borde ha upptäckt vid undersökningen, såvida inte säljaren har handlat i strid mot tro och heder.[33] Därmed kan riskfördelningen omfördelas om köparen företar en undersökning alternativt underlåter att företa en undersökning. Således åläggs köparen vid ett företagsförvärv en undersökningsplikt. Det ska dock poängteras att det inte rör sig om någon plikt i egentlig mening eftersom undersökningen företas i köparens intresse och följden av en utebliven undersökning är endast att köparen förlorar rätten att åberopa fel som hen borde ha upptäckt vid en sådan undersökning. Undersökningsplikt är dock den terminologi som normalt används i detta sammanhang.[34] Omfattningen av köparens undersökningsplikt beror på vad som kan krävas av en person i köparens ställning, vad köparen borde upptäcka avgörs därmed utifrån omständigheterna i varje enskilt fall.[35] För att minska risken för rättsliga anspråk från köparen ligger det därför i säljarens intresse att tillgängliggöra så mycket material som möjligt.

2.3 Informationshantering vid due diligence

Informationshanteringen innebär som regel att uppgifter om målföretaget väljs ut och överförs från säljaren till köparen via mellanhänder, ofta en advokatbyrå.[36] Mottagaren av informationen kan vanligtvis inte använda informationen hur de vill utan användningen regleras i de flesta fall av sekretessavtal mellan köpare och säljare.[37] Sekretessavtalet har två huvudsakliga syften, dels att förhindra utlämnande av känslig information till tredjeman och dels att förhindra att motparten använder sig av den känsliga informationen för egen vinning. Därmed kan inte en säljare låta en köpare påbörja sin due diligence-undersökning utan att ett sekretessavtal är på plats.[38] Det finns ingen särskild lag som reglerar sekretessavtal, vilket innebär att AvtL och allmänna kontraktsrättsliga principer blir tillämpliga på ett sekretessavtal. Således har parterna friheten att utforma sekretessavtalet och därigenom

[32] 20 § 1st. KöpL.
[33] 20 § 2st. KöpL.
[34] Ramberg(1992) s.173.
[35] Prop 1988/89:76 s.94.
[36] Sevenius(2013) s.353.
[37] Ibid. s.363.
[38] Forssman(2016) s.24.

gränserna för informationsanvändningen på det sätt de finner lämpligt.[39] Dessutom finns tystnadsplikter i lagstiftningen som sätter yttre gränser för hur informationen får användas, bland annat i lagen om skydd för företagshemligheter (1990:409), GDPR, konkurrenslagen(2008:579) och marknadsmissbrukslagen(2016:1307).[40] Olika typer av information aktualiserar de olika lagarna, med hänsyn till att uppsatsen är avgränsad till att endast fokusera på personuppgifter är det enbart information i form av personuppgifter och kopplingen till GDPR som kommer att behandlas i uppsatsens fortsatta framställning.[41] I de flesta due diligence-förfaranden förekommer personuppgifter i olika former, personuppgifter om ledande befattningshavare, nyckelpersoner, andra medarbetare och personuppgifter i kundregister är vanligt förekommande.[42]

Förmedlingen av information sker genom att informationen tillgängliggörs i ett så kallat datarum. Det finns två olika typer av datarum, manuella datarum och virtuella datarum. I ett manuellt datarum finns all information som säljaren gjort tillgänglig för köparen i fysisk form, köparen och dess representanter får sedan gå igenom materialet i det rum där det gjorts tillgängligt. I takt med att dokumentationen i de flesta företagen har blivit digitaliserad och att priserna för virtuella datarum har sjunkit används manuella datarum i dagsläget i mycket begränsad utsträckning.[43] I ett virtuellt datarum läggs dokumentationen istället upp digitalt via en datarumsleverantör. Det virtuella datarummet möjliggör att de inblandade parterna får en bra kontroll över vilket material som finns tillgängligt samt vem som har tittat på vad. Dessutom är det enkelt att uppdatera ett virtuellt datarum och det kan vara ett obegränsat antal användare inne samtidigt.[44] Vidare innehåller virtuella datarum funktioner som stödjer och underlättar analysarbetet. Dokumentationen i virtuella datarum numreras, kategoriseras och görs sökbar med så kallad booelsk sökning vilket innebär sökning med kommandona "och" "eller" och "inte".[45] Det finns ingen fastställd standard för hur mycket information eller vilken information som ska finnas i ett datarum. Kvaliteten på informationen tenderar att variera och en del av informationen kan därmed vara relativt intetsägande eller irrelevant för en viss köpare.[46] För att få tillträde till datarummet krävs vanligtvis att

[39] Tonell(2012) s.14.
[40] Sevenius(2013) s.363.
[41] Se avsnitt 1.6.
[42] Sevenius(2013) s.368.
[43] Forssman(2016) s.32.
[44] Ibid. s.35.
[45] Sevenius(2017) s.2.
[46] Sevenius(2013) s.141.

besiktningskonsulterna intygar att de ska följa vissa regler. Den mest centrala regeln är att dessa ska behandla all information konfidentiellt. Säljare och köpare brukar som nämnts ovan ingå ett sekretessavtal till vilka de vanligtvis har med en klausul där de förpliktas att se till att de rådgivare som de anlitar binds av motsvarande sekretessvillkor, en så kallad *back-to-back clause*.[47]

2.4 Aktörerna i en due diligence

Ett företagsförvärv kan, på ett förenklat sätt, beskrivas som en situation då ett företag köper ett företag av ett annat företag.[48] Därmed innefattar ett företagsförvärv i de flesta fall en köpare och en säljare med ett målbolag. Utöver dessa aktörer tillkommer en rad olika ombud till både köpare och säljare som till exempel investmentbanker, advokatbyråer och revisionsbyråer.[49] För den här uppsatsen är det givetvis advokatbyråerna som är det centrala ombudet. Vid ett företagsförvärv anlitar köparen en advokatbyrå och säljaren en annan advokatbyrå. Som tidigare nämnts används ett virtuellt datarum i de allra flesta due diligence-processer. Datarummen manövreras av en utomstående aktör och följaktligen tillkommer ytterligare en aktör i due diligence-processen, nämligen datarumsleverantören. Det finns flera företag som arbetar med att sätta upp datarum för due diligence-processer. *Merrill corporation*[50] och *Imprima*[51] är två leverantörer som är ledande på marknaden för datarumsleverantörer.

[47] Sevenius(2013) s.141-f.
[48] Sevenius(2011) s.32.
[49] Sevenius(2013) s.15-ff.
[50] Merrill Corporation.
[51] Imprima.

3. GDPR

3.1 Inledning

Beslutet om att införa GDPR antogs den 27 april 2017 efter flera år av intensivt förhandlande mellan EU:s medlemsstater.[52] GDPR trädde sedan i kraft den 25 maj 2018. Före införandet av GDPR reglerades hantering av personuppgifter i Sverige av personuppgiftslagen(1998:204), PuL.

Redan i artikel 1 GDPR anges förordningens två grundläggande syften. GDPR syftar till att skydda fysiska personer när det kommer till behandling av personuppgifter samt att skapa förutsättningar för det fria flödet av personuppgifter inom unionen. Syftet är därmed att skapa en konformitet inom unionen vad gäller skyddet för personuppgifter. Det tidigare gällande dataskyddsdirektivet medförde att medlemsstaternas regler för skydd av personuppgifter kunde se mycket olika ut, ett problem som GDPR syftar till att lösa.[53]

I skälen till GDPR hänvisas till det den grundläggande rättigheten till skydd av personuppgifter som föreskrivs i artikel 8 EU-stadgan[54], vilket kan sägas vara grunden för hela GDPR. Vidare anges i skälen till GDPR att behandling av personuppgifter bör utformas på ett sätt som gör att den tjänar människor[55], ett stadgande som medför att det inte enbart är individers integritet som ska skyddas vid behandling av personuppgifter.[56] Dessutom anges att rätten till skydd för personuppgifter inte är en absolut rättighet, utan den ska förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i överensstämmelse med proportionalitetsprincipen.[57] GDPR beaktar därför alla de grundläggande rättigheterna, friheterna och principerna som anges i EU-stadgan.

[52] Frydlinger m.fl.(2018) s.28.
[53] IT Governance Privacy Team(2016) s.2.
[54] GDPR skäl 1.
[55] GDPR skäl 4.
[56] Frydlinger m.fl.(2018) s.30.
[57] GDPR skäl 4.

3.2 Tillämpningsområde

3.2.1 Materiellt tillämpningsområde

I artikel 2.1 GDPR stadgas förordningens materiella tillämpningsområde. GDPR ska tillämpas på behandling[58] av personuppgifter[59] som helt eller delvis sker på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register.[60] Således omfattas all typ av automatisk behandling, oavsett om den automatiska delen av behandlingen endast är partiell.[61] Behandling som inte sker på automatisk väg omfattas alltjämt av GDPR:s tillämpningsområde förutsatt att personuppgifterna i fråga ingår eller är avsedda att ingå i ett register.[62] Med register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier.[63] Vid uppsättning av ett datarum torde personuppgifterna, oavsett om det är ett manuellt eller virtuellt datarum, vara strukturerade och tillgängliga enligt särskilda kriterier. GDPR:s tillämpningsområde är därmed teknikneutralt och det går därför inte att, i en due diligence, behandla personuppgifter på annan än automatisk väg i syfte att kringgå reglerna i GDPR förutsatt att personuppgifterna ingår eller är tänkta att ingå i ett register.

Det ska dock tilläggas att det finns flera undantag som gör att vissa typer av behandling faller utanför GDPR:s tillämpningsområde. Det mest centrala undantaget avser privat behandling av personuppgifter.[64] Med privat behandling avses fysiska personers behandling av personuppgifter som är hänförlig till verksamhet som helt och hållet är privat eller har samband med personens hushåll och därmed saknar koppling till yrkes eller affärsmässig verksamhet.[65] Vidare undantas behöriga myndigheters behandling avseende uppgifter om brott eller annars inom rättsväsendet[66], sådan behandling regleras istället i en särskild unionsakt.[67] Dessutom undantas sådan behandling som är hänförlig till verksamhet som ej omfattas av unionsrätten.[68] Slutligen anges att GDPR inte ska påverka tillämpningen av EU:s

[58] Se definition i avsnitt 3.3.2.
[59] Se definition i avsnitt 3.3.1.
[60] Art 2.1 GDPR.
[61] Frydlinger m.fl.(2018) s.63.
[62] Skäl 15 i GDPR.
[63] Art 4.6 GDPR.
[64] Art 2.2 c GDPR.
[65] Skäl 18 i GDPR.
[66] Skäl 19 i GDPR.
[67] Europaparlamentets och rådets direktiv (EU) 2016/680.
[68] Art 2.2. a GDPR.

direktiv[69] om elektronisk handel avseende tjänsteleverérande mellanhänders ansvar.[70] Inget av ovanstående undantag är dock tillämpliga vid informationshanteringen i samband med en due diligence.

3.2.2 Territoriellt tillämpningsområde

Den svaga svenska kronan har medfört ett ökat intresse från utländska aktörer avseende den svenska företagsförvärvsmarknaden, vilket ifjol visade sig genom att antalet utländska köp av svenska bolag ökade med 20 procent. Thomas Westin, nordenchef på Barclays, anger vidare att det starka intresset framförallt kommer från asiatiska och amerikanska aktörer.[71] Dessutom skulle en ”no-deal”-Brexit innebära att bolag från Storbritannien anses vara utanför EU.[72] Det finns därför faktorer som talar för att aktiviteten för länder som befinner sig utanför EU kommer att öka på den svenska företagsförvärvsmarknaden. Därmed är det viktigt att vara införstådd i GDPR:s territoriella tillämpningsområde.

Det territoriella tillämpningsområdet regleras av artikel 3 GDPR och är uppdelat i två delar. Den ena gruppen är personuppgiftsansvariga och personuppgiftsbiträden som är etablerade inom EU, oavsett om själva personuppgiftsbehandlingen sker inom EU eller ej.[73] Dessutom tillkommer personuppgiftsansvariga och personuppgiftsbiträden som är etablerade utanför EU men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.[74] Den andra gruppen omfattar personuppgiftsansvariga och personuppgiftsbiträden som är etablerade utanför unionen men där de registrerade befinner sig inom unionen. För att den andra gruppen ska omfattas krävs vidare att ett av följande två kriterier är uppfyllda: antingen ska behandlingen ha anknytning till utbjudande av varor eller tjänster till registrerade i unionen, oavsett om de erbjuds kostnadsfritt eller ej, alternativt ska behandlingen avse övervakning av deras beteende så länge beteendet sker inom unionen.[75] Det bör noteras att GDPR inte gör någon åtskillnad mellan personuppgiftsansvarig och personuppgiftsbiträde vad gäller det territoriella tillämpningsområdet.[76] Således kan det konstateras att det territoriella

[69] Europaparlamentets och rådets direktiv 2000/31/EG.
[70] Art 2.4 GDPR.
[71] Höiseth(2019).
[72] EDPB, *Infonote nodeal brexit.*
[73] GDPR art 3.1.
[74] GDPR art 3.3.
[75] GDPR art 3.2.
[76] Voigt och von dem Bussche s.22.

tillämpningsområdet sträcker sig över hela världen, och vilken organisation som helst kan bli föremål för tillämpning av GDPR givet att ovan angivna förutsättningar föreligger.

3.3 Grundläggande begrepp

I följande avsnitt redogörs för ett antal begrepp som har stor betydelse för flera bestämmelser i GDPR. Definitionerna av de olika begreppen återfinns i artikel 4 GDPR och kommer att förklaras närmare nedan.

3.3.1 Personuppgifter

Personuppgift är det mest centrala begreppet i GDPR. Förordningen är endast tillämplig på behandling av data som rör personuppgifter.

Personuppgift definieras i artikel 4.1 GDPR enligt följande:

> ”varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.”[77]

Följaktligen är det ett mycket vitt begrepp. Begreppet omfattar samtliga typer av uppgifter som kan härledas till fysiska personer och personer i alla positioner. Dessutom omfattas indirekta uppgifter. Med indirekta uppgifter avses uppgifter som i kombination med andra uppgifter kan användas för att identifiera en person.[78] Uppgifter om juridiska personer, uppgifter om avlidna och uppgifter som varken direkt eller indirekt kan hänföras till en person omfattas dock inte av begreppet personuppgifter.[79] Således kan personuppgifter exempelvis vara en persons namn, identifieringsnummer som exempelvis personnummer, lokaliseringsuppgifter[80] samt online-identifikatorer som till exempel cookies[81] och IP-

[77] Art 4.1 GDPR.
[78] Frydlinger m.fl.(2018) s.45.
[79] Skäl 14, 26 och 27 i GDPR.
[80] *Lokaliseringsuppgifter* är sådana uppgifter som exempelvis uppstår vid användning av appar i mobilen som använder och registrerar platsdata eller vid körning av smarta bilar.
[81] *Cookies* är en kort text som lagras i en besökares webbläsare när hen besöker webbsidor.

nummer.[82] Informationen i en due diligence innefattar i många fall uppgifter om ledande befattningshavare, nyckelpersoner och andra medarbetare exempelvis i form av anställningsavtal.[83] Dessutom är det vanligt att det förekommer uppgifter om kunder, exempelvis i olika kundregister. Med hänsyn till ovanstående definition torde det inte råda något tvivel om att sådana uppgifter är att se som personuppgifter i förordningens mening och att GDPR därmed är tillämplig på en del av den information som är vanligt förekommande vid en due diligence.

Personuppgifter kan vidare delas in i två huvudsakliga kategorier, generella personuppgifter och särskilda kategorier av personuppgifter som också benämns känsliga personuppgifter. Generella personuppgifter omfattar samtliga personuppgifter. Känsliga personuppgifter är en del av de generella personuppgifterna och omfattar, enligt artikel 9.1 GDPR, personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, behandling av genetiska uppgifter, biometriska uppgifter för att identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Behandling av känsliga personuppgifter är förbjuden såvida inte något av undantagen för behandling av känsliga personuppgifter är uppfyllt.[84] Artikel 9.2 GDPR anger en rad olika undantag då känsliga personuppgifter tillåts behandlas, varav en del av undantagen är utformade på så sätt att de ger utrymme för nationell reglering vilket i svensk rätt har aktualiserats genom 3 kap lag med kompletterande bestämmelser till EU:s dataskyddsförordning(2018:218), dataskyddslagen. Bestämmelserna i 3 kap dataskyddslagen anger dock inte något undantag som går ut över de som anges i GDPR. Däremot förtydligas de undantag som anges i GDPR genom 3 kap dataskyddslagen.

3.3.2 Personuppgiftsbehandling

När det har fastställts att det är fråga om personuppgifter är nästa steg att fastställa om det rör sig om personuppgiftsbehandling i förordningens mening.

Definitionen av personuppgiftsbehandling framgår av artikel 4.2 GDPR:

[82] Voigt och von dem Bussche(2017) s.11.
[83] Sevenius(2013) s.368.
[84] Art 9.1 GDPR.

> ”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,”[85]

Som framgår av ovanstående definition är begreppet brett definierat och omfattar samtliga delar av en normal informationsbehandling såsom insamling, bearbetning, lagring och radering. Därmed omfattas i princip alla åtgärder som vidtas avseende personuppgifter. Syftet med den vida definitionen är att förhindra kringgående av GDPR samt för att göra tillämpningsområdet oberoende av teknisk utveckling.[86] Definitionen av personuppgiftsbehandling begränsas dock, som tidigare nämnts, av artikel 2.1 GDPR genom att behandling som inte är automatisk endast omfattas om personuppgifterna i fråga ingår eller är tänkta att ingå i ett register.[87] GDPR innehåller ingen skillnad mellan strukturerade och ostrukturerade personuppgifter vilket är en skillnad från den tidigare gällande PuL. Strukturerade personuppgifter är personuppgifter som ingår i en sammanställning av information vilken underlättar sökningar, exempelvis i en databas. Ostrukturerade personuppgifter är istället personuppgifter som ingår i ostrukturerat material, exempelvis i löpande text.[88] Förändringen medför därför en utvidgning av begreppet personuppgiftsbehandling sett ur ett svenskt perspektiv.[89]

Informationshanteringen i samband med en due diligence kan gå till på olika sätt, exempelvis genom att informationen behandlas via ett virtuellt eller manuellt datarum. Oavsett vilket typ av datarum som används innebär informationshanteringen, med hänsyn till ovanstående definition, en personuppgiftsbehandling enligt GDPR.

[85] Art 4.2 GDPR.
[86] Voigt och von dem Bussche(2017) s.9-f.
[87] Se avsnitt 3.2.1.
[88] Prop. 2005/06:173 Översyn av personuppgiftslagen s.24.
[89] Frydlinger m.fl.(2018) s.47.

3.3.3 Personuppgiftsansvarig

Det är centralt att definiera den personuppgiftsansvarige eftersom de absolut flesta skyldigheterna enligt GDPR åligger denne. Därmed inleds i många fall den juridiska analysen med att fastställa vem som är personuppgiftsansvarig.[90]

Artikel 4.7 GDPR definierar personuppgiftsansvarig enligt följande:

> ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.”[91]

Definitionen kan delas upp i tre olika komponenter: 1) En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ 2) som ensamt eller tillsammans med andra 3) bestämmer ändamålen och medlen för behandlingen av personuppgifter.[92] Den personuppgiftsansvariges legala form är inte avgörande för om denne ska anses ansvarig för de förpliktelser som GDPR medför. Det bör även noteras att GDPR inte har något undantag för koncerner, utan varje entitet inom en koncern är ensamt ansvarig.[93] Vid varje personuppgiftsbehandling finns det minst en personuppgiftsansvarig, det behöver dock inte nödvändigtvis endast vara en personuppgiftsansvarig utan ansvaret kan delas av flera gemensamt. Gemensamt ansvar föreligger enligt artikel 26 GDPR i de fall då två eller flera personuppgiftsansvariga fastställer ändamålen och medlen för behandlingen.[94] När ansvaret är gemensamt behöver de gemensamt ansvariga tillgodose en tydlig fördelning av ansvaret mellan varandra.[95] Med rätten att bestämma ändamålen och medlen för behandlingen menas bestämmanderätten över hur och varför en behandling utförs. Just varför behandlingen utförs samt vem som har tagit initiativ till behandlingen är centrala omständigheter när graden av bestämmande ska avgöras. Vem eller vilka som har bestämmanderätten över en viss behandling avgörs utifrån vilka faktiska omständigheter som föreligger i varje enskilt fall.[96] Enligt artikel 29-gruppen kan rätten att bestämma över personuppgifter bero på följande

[90] Frydlinger m.fl.(2018). s.51.
[91] Art 4.7 GDPR.
[92] Voigt och von dem Bussche(2017). s.17.
[93] Ibid. s.18.
[94] Art 26.1 GDPR.
[95] Voigt och von dem Bussche(2017). s.18.
[96] Artikel 29-gruppen, WP 169, s.13.

omständigheter: uttrycklig behörighet, underförstådd behörighet eller faktiskt inflytande.[97] Med uttrycklig behörighet avses att bestämmanderätten framgår av lagtext. Underförstådd behörighet är behörighet som ej finns uttryckt i lagtext men som grundar sig i rättsliga bestämmelser eller i rättspraxis, som till exempel en arbetsgivares ansvar för en anställds personuppgifter.[98] Vid faktiskt inflytande grundas bestämmanderätten på de faktiska omständigheterna. Vanligtvis baseras det faktiska inflytandet på avtal och annan dokumentation som rör förhållandet mellan de inblandade aktörerna.[99] Dessutom är det viktigt att ha i åtanke att det inte är möjligt att avtala bort ansvaret, om det visar sig att den egentliga bestämmanderätten över personuppgiftsbehandlingens syfte ligger hos en viss personuppgiftsansvarig har ett avtal som föreskriver något annat ingen betydelse.[100]

Aktörerna i en due diligence innefattar köpare med ombud samt säljare med målbolag och ombud, därtill kommer även datarumsleverantören. Alla dessa aktörer är på något sätt inblandade i den personuppgiftsbehandling som sker vid en due diligence och innehar därmed rollen som antingen personuppgiftsansvarig eller personuppgiftsbiträde. I samband med en due diligence kan det konstateras att samtliga aktörer uppfyller det första rekvisitet för att anses vara personuppgiftsansvarig eftersom alla är juridiska personer. Med hänsyn till att, som nämnts ovan, omständigheterna i varje enskilt fall avgör vem som ska anses ha bestämmanderätt över behandlingen och anses vara personuppgiftsansvarig är det inte möjligt att fastslå vem eller vilka aktörer som företar rollen som personuppgiftsansvarig vid informationshanteringen i samband med en due diligence. Däremot kan det generellt sett sägas att köpare och säljare med respektive ombud i regel har bestämmanderätt över ändamålen och medlen för delar av personuppgiftsbehandlingen. Bestämmanderätten föreligger i sådana fall mot bakgrund av *faktiskt inflytande.* Avtal och annan dokumentation som föreskriver *faktiskt inflytande* skulle exempelvis kunna vara de uppdragsavtal som ingås mellan advokatbyrå och köpare eller säljare vid en due diligence vilka bland annat anger advokatbyråernas behörighet att hantera den tillgängliga informationen.

[97] Artikel 29-gruppen, WP 169, s.10-f.
[98] Ibid. s.10.
[99] Ibid. s.11.
[100] Frydlinger m.fl.(2018) s.51.

3.3.4 Personuppgiftsbiträde

I takt med att fler och fler företag outsourcar personuppgiftsbehandlingen och på grund av ökad tillgänglighet av molntjänstleverantörer blir det fler och fler aktörer som intar rollen som personuppgiftsbiträde.[101]

Personuppgiftsbiträde definieras i artikel 4.8 GDPR som:

> ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,”[102]

Således beror existensen av ett personuppgiftsbiträde på ett beslut taget av den personuppgiftsansvarige om huruvida behandling av personuppgifter sker inom organisationen eller om behandlingen delegeras till en extern organisation. I det fall att behandlingen delegeras externt blir den organisationen ett personuppgiftsbiträde.[103] Delegering av personuppgiftsbehandling externt är som nämnts ovan vanligt förekommande i due diligence-processer när en datarumsleverantör anlitas för att hantera information.

Artikel 29-gruppen har ställt upp två kriterier för att en entitet ska anses vara ett personuppgiftsbiträde. Dels att det ska vara en separat fysisk eller juridisk person i förhållande till den personuppgiftsansvarige och dels att denne behandlar personuppgifter för den personuppgiftsansvariges räkning. Just att personuppgiftsbiträdet *endast* utför personuppgiftsbehandlingen för den personuppgiftsansvariges räkning är väsentligt i det här sammanhanget. I händelse av att personuppgiftsbiträdet går utöver sitt mandat eller får alltför stort inflytande över bestämmandet av behandlingens syfte och medel blir personuppgiftsbiträdet istället att se som personuppgiftsansvarig.[104] När ett personuppgiftsbiträde har identifierats ska den personuppgiftsansvarige ingå ett skriftligt avtal med det aktuella personuppgiftsbiträdet, ett så kallat personuppgiftsbiträdesavtal. GDPR ställer dessutom upp flera krav på vad ett sådant avtal ska innehålla.[105] Vid fastställande av om en entitet ska anses vara personuppgiftsbiträde är det faktiska förhållandet avgörande, inte vad som står i ett eventuellt personuppgiftsbiträdesavtal.[106]

---

[101] Frydlinger m.fl.(2018) s.56.
[102] Art 4.8 GDPR.
[103] Voigt och von dem Bussche(2017) s.20.
[104] Art 29-arbetsgruppen, WP 169, s.25.
[105] Art 28.3 GDPR.
[106] Frydlinger m.fl.(2018) s.56.

En datarumsleverantör är en separat juridisk person i förhållande till den som är personuppgiftsansvarig vid en due diligence. Vidare innebär tillhandahållande av datarum där personuppgifter återfinns en personuppgiftsbehandling enligt GDPR.[107] Således behandlar datarumsleverantören personuppgifter för den personuppgiftsansvariges räkning. Därmed kan det konstateras att datarumsleverantören innehar rollen som personuppgiftsbiträde vid en due diligence där ett virtuellt datarum används så länge inte datarumsleverantören går utöver sitt mandat och får alltför stort inflytande över behandlingens syfte och medel. Den som är personuppgiftsansvarig måste därför ingå ett personuppgiftsbiträdesavtal med datarumsleverantören.

3.3.5 Personuppgiftsansvariges och personuppgiftsbiträdets ansvar

Varje personuppgiftsansvarig som har medverkat vid behandlingen ansvarar för skada som orsakats av en behandling som strider mot GDPR. Ett personuppgiftsbiträde ansvarar för skada som uppkommit till följd av behandlingen endast om denne inte har fullgjort de skyldigheter i GDPR som specifikt riktar sig till personuppgiftsbiträden eller om denne agerat utanför eller i strid med de lagenliga anvisningar som den personuppgiftsansvarige har lämnat.[108] Vidare är ansvaret mellan personuppgiftsansvariga och personuppgiftsbiträden solidariskt,[109] vilket innebär att varje personuppgiftsansvarig och eller personuppgiftsbiträde kan hållas ansvarig för hela skadan. Således kan en registrerad person som har blivit utsatt för skada vända sig till vem som helst av ovanstående aktörer. GDPR innehåller dessutom en bestämmelse om regressrätt vilken anger att den part som har blivit tvungen att betala full ersättning för uppkommen skada har rätt att återkräva de andra parterna på den del av skadan som avser deras ansvar.[110]

[107] Se avsnitt 3.3.2.
[108] Art 82.2 GDPR.
[109] Art 82.4 GDPR.
[110] Art 82.5 GDPR.

3.4 Behandling av personuppgifter

3.4.1 Inledning

I olika organisationer finns det olika typer av registrerade. Det finns dock två huvudsakliga typer av registrerade som är vanligt förekommande i de flesta organisationer. Kunder som finns i olika kundregister samt anställda.[111] Personuppgifters livscykel inom en organisation kan vidare delas upp i tre övergripande faser: personuppgifterna kommer in till organisationen, personuppgifterna behandlas av organisationen samt personuppgifterna raderas av organisationen.[112] Vid utförandet av en due diligence är det den andra fasen, behandling av personuppgifter, som är mest relevant.

3.4.2 Laglig personuppgiftsbehandling

Rättslig grund är en förutsättning för att en personuppgiftsansvarig ska få behandla personuppgifter. Vid avsaknad av rättslig grund är en personuppgiftsbehandling ej förenlig med GDPR. De rättsliga grunderna för personuppgiftsbehandling anges i artikel 6.1 GDPR. Förordningen åtskiljer två olika typer av situationer då den personuppgiftsansvarige har rättslig grund för att behandla personuppgifter. Den ena situationen är när de registrerade har lämnat samtycke till behandlingen.[113] Den andra situationen är när de registrerade inte lämnat samtycke men där behandlingen anses nödvändig för att den personuppgiftsansvarige ska kunna utföra vissa angivna åtgärder.[114]

3.4.2.1 Samtycke som rättslig grund

Enligt artikel 4.11 GDPR definieras samtycke som:

> ”av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.”[115]

Samtycket ska alltså vara frivilligt, specifikt, informerat och vara en otvetydig viljeyttring. Ett samtycke anses inte vara frivilligt om de registrerade inte har något verkligt val, känner

[111] Frydlinger m.fl.(2018) s.134.
[112] Ibid. s.135.
[113] Art 6.1 a GDPR.
[114] Art 6.1 b-f. GDPR.
[115] Art 4.11 GDPR.

sig tvungna att samtycka eller om de får utstå negativa konsekvenser om de ej samtycker.[116] Vid en due diligence kan det förekomma situationer där en arbetsgivare söker behandla en anställds personuppgifter baserat på samtycke. Med hänsyn till den maktobalans som råder mellan en arbetsgivare och en anställd kan dock ett sådant samtycke vara problematiskt eftersom det kan vara svårt att fastställa att ett sådant samtycke har lämnats på frivillig basis.[117] Att samtycket ska vara specifikt innebär att det måste lämnats i förhållande till ett eller flera specifika syften och att de registrerade har ett val i relation till dessa syften.[118] För att samtycket ska anses vara informerat krävs att de registrerade har fått information före samtycket lämnas.[119] Med en otvetydig viljeyttring avses att samtycket alltid måste lämnas genom att de registrerade utför en aktiv handling, dessutom måste det vara uppenbart att de registrerade har samtyckt till den särskilda behandlingen.[120] Därmed anses inte tystnad, inaktivitet eller på förhand ikryssade rutor vara ett giltigt samtycke.[121]

Vidare anger artikel 7 GDPR ytterligare förutsättningar gällande samtycket. För det första är det den personuppgiftsansvarige som har bevisbördan för att samtycke föreligger, denne måste alltså kunna visa att de registrerade har samtyckt till behandling av deras personuppgifter.[122] Vidare krävs, i de fall då samtycke lämnas genom skriftlig förklaring som också rör andra frågor till exempel vid ett avtal, att frågan om samtycke särskiljs från de andra frågorna samt att samtyckesfrågan förklaras på ett begripligt och lättillgängligt sätt med ett klart och tydligt språk. Strider förklaringen i någon del mot GDPR ska den delen inte anses vara bindande.[123] Dessutom ska de registrerade äga rätt att återkalla samtycket, återkallande av samtycket ska vara lika lätt som lämnande av samtycke.[124] Det sista villkoret innebär att vid bedömning av om samtycket lämnats frivilligt ska det särskilt beaktas om ett avtals genomförande varit beroende av samtycke men ej varit nödvändigt för att fullgöra avtalet.[125] I det fall att samtycket ska ligga till grund för behandling av känsliga personuppgifter krävs dessutom att samtycket har lämnats uttryckligen.[126]

---

[116] Art 29-arbetsgruppen, WP 259, s.5.
[117] Ibid. s.7.
[118] Ibid. s.11.
[119] Ibid. s.13.
[120] Ibid. s.15.
[121] Skäl 32 i GDPR.
[122] Art 7.1 GDPR.
[123] Art 7.2 GDPR.
[124] Art 7.3 GDPR.
[125] Art 7.4 GDPR.
[126] Art 9.2 a GDPR.

3.4.2.2 Nödvändighet som rättslig grund

Kravet på nödvändighet förklaras ej i GDPR, vilket det inte heller gjordes i det tidigare gällande dataskyddsdirektivet. Däremot kan viss vägledning angående tolkning av begreppet återfinnas i förarbeten och praxis. Nödvändighetsrekvisitet innebär inget krav på att det ska vara omöjligt att fullgöra förpliktelsen eller utföra uppgiften utan att behandlingsåtgärden vidtas.[127] Vidare finns det ett mål från EU-domstolen där de tolkar begreppet *nödvändighet* i det tidigare gällande dataskyddsdirektivet. EU-domstolen kommer i det målet fram till att kravet på att behandlingen ska vara nödvändig för ändamålet inte innebär att behandlingsåtgärden ska vara oundgänglig, utan behandlingen kan anses vara nödvändig om den leder till effektivitetsvinster.[128] Domen rörde visserligen, som tidigare nämnts, nödvändighetsrekvisitet i dataskyddsdirektivet, men domen bör kunna användas även för att tolka GDPR.[129] Domen ger således stöd för tolkningen om att det ej finns ett krav på att det ska vara omöjligt att utföra uppgiften utan att behandlingsåtgärden vidtas.

De åtgärder som anges, utöver samtycke, är uttömmande vilket medför att någon av de angivna åtgärderna måste vara tillämplig för att behandlingen ska vara laglig i avsaknad av samtycke.[130] De åtgärder som anges är i viss mån överlappande vilket medför att flera av grunderna kan vara tillämpliga samtidigt avseende en och samma personuppgiftsbehandling.[131] Först och främst anges att behandlingen är laglig om den är *nödvändig* för att fullgöra ett avtal som de registrerade är part i alternativt för att vidta åtgärder på begäran av de registrerade innan ett sådant avtal ingås.[132] Behandlingen är vidare laglig om den är *nödvändig* för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som åvilar denne.[133] Sådana rättsliga förpliktelser kan följa av lag, förordningar eller andra föreskrifter. Dessutom kan rättsliga förpliktelser följa av domar, myndighetsbeslut och kollektivavtal.[134] Behandlingen är vidare laglig om den är *nödvändig* för att skydda intressen som är av väsentlig betydelse för de registrerade eller annan fysisk person.[135]

---

[127] SOU 2017:39 *Datsskytddsutredningen.* s.105.
[128] Karnov internet, artikel 6 GDPR, not 68. och mål C-524/06.
[129] Prop 2017/18: 105, *Ny dataskyddslag.* s.47.
[130] Ibid. s.46.
[131] SOU 2017:39, *Dataskyddsutredningen,* s.104.
[132]Art 6.1 b GDPR.
[133]Art 6.1 c GDPR.
[134] Prop 2017/18:105, *Ny dataskyddslag.* s.52.
[135] Art 6.1 d GDPR.

Behandlingen är även laglig om den är *nödvändig* för att utföra en uppgift av allmänt intresse eller som en del av den personuppgiftsansvariges myndighetsutövning.[136]

Slutligen anses behandling vara laglig om den är *nödvändig* för ändamål som avser den personuppgiftsansvariges eller en tredjeparts berättigade intressen, såvida inte de registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter.[137] Den sistnämnda grunden innebär således en intresseavvägning mellan den personuppgiftsansvariges och de registrerades intressen och fungerar som en generalklausul på så sätt att den kan användas om det inte finns någon annan rättslig grund som är tillämplig.[138] Intresseavvägningen kan delas upp i fyra olika moment:[139]

1. *Identifiera de aktörer vars intressen involveras i behandlingen.*

Till att börja med måste de relevanta aktörerna och deras intressen identifieras. Vanligtvis är aktörerna enbart den personuppgiftsansvarige och de registrerade men även andra parters intressen kan aktualiseras vilket exempelvis var fallet i mål C-131/12.[140]

2. *Identifiera om den personuppgiftsansvarige eller tredje part har ett berättigat intresse.*

För att ett intresse ska anses vara *berättigat* krävs att intresset är lagenligt vilket betyder att det måste överensstämma med tillämplig EU-lagstiftning och nationell lagstiftning. Vidare måste intresset vara tillräckligt tydligt formulerat för att en intresseavvägning ska kunna genomföras. Dessutom måste intresset vara ett verkligt och nuvarande intresse, det är alltså inte möjligt att grunda intresseavvägningen på ett framtida eller hypotetiskt intresse.[141]

3. *Identifiera om och i vilken grad de registrerades intressen eller rättigheter påverkas av behandlingen.*

Vid bedömning av de registrerades intressen och rättigheter finns det ett antal faktorer som har betydelse. Mängden personuppgifter som behandlas, vad det är för typ av personuppgifter samt vad personuppgifterna ska användas till är alla faktorer som ska beaktas vid

[136] Art 6.1 e GDPR.
[137] Art 6.1 f GDPR.
[138] Holtz(2019).
[139] Frydlinger m.fl.(2018) s.143.
[140] Ibid.
[141] Artikel 29-gruppen, WP 217, s.25.

bedömningen av de registrerades intressen och rättigheter.[142] Vidare ska en sådan bedömning innefatta huruvida de registrerade vid tidpunkten för inhämtandet av personuppgifter rimligen skulle kunna förvänta sig att en personuppgiftsbehandling för det aktuella ändamålet skulle kunna komma att ske.[143]

4. *Övergripande avvägning mellan intressen.*

Det sista momentet handlar om att göra en helhetsbedömning av ovanstående intressen. Helhetsbedömningen går ut på att bedöma för vem det "kostar" mest att behandla respektive inte behandla personuppgifter. Kostnader och effektivitetsförluster för den personuppgiftsansvarige vägs mot den negativa påverkan som behandlingen kan innebära för de registrerade. Dessutom ska det beaktas vilka ytterligare åtgärder den personuppgiftsansvarige ämnar vidta för att skydda de registrerade och deras personuppgifter.[144]

3.4.3 De registrerades rättigheter

3.4.3.1 Säkerhet i samband med behandlingen

I artikel 5.1 f GDPR föreskrivs principen om integritet och konfidentialitet vilken tar sikte på informationssäkerhet och innebär att den personuppgiftsansvarige eller personuppgiftsbiträdet måste säkerställa en lämplig säkerhet för behandling av personuppgifter.[145] Det finns ingen närmare förklaring på vad som menas med en *lämplig säkerhet* eller vilken nivå av säkerhet som krävs. Principen föreskriver endast att det ska finnas en lämplig säkerhet samt vilka mål som ska uppnås genom säkerheten. För att få en tydligare bild över vilken säkerhet det är som åsyftas kan principen läsas tillsammans med artikel 32 GDPR och skäl 78 till GDPR.[146] Enligt artikel 32 GDPR ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Hänsyn ska tas till den tekniska utvecklingen, genomförandekostnader samt behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers

[142] Frydlinger m.fl.(2018) s.145.
[143] Skäl 47 i GDPR.
[144] Frydlinger m.fl.(2018) s.145.
[145] Art 5.1 (f). GDPR.
[146] Frydlinger m.fl.(2018) s.259.

rättigheter och friheter.[147] En väsentlig beståndsdel av ett företags säkerhetspolicy är således att, om möjligt, förhindra överträdelser av GDPR och om en överträdelse trots allt skulle uppstå ska den ansvarige kunna agera snabbt.[148] Vidare anges i skäl 78 att den personuppgiftsansvarige ska anta interna strategier och vidta åtgärder, i synnerhet genom att beakta principerna i artikel 25 GDPR om inbyggt dataskydd och dataskydd som standard. Dessutom anges följande förslag på åtgärder: minimering av personuppgiftsbehandling, pseudonymisering av personuppgifter, vidtagande av öppenhet angående personuppgifternas syfte och behandling samt ge de registrerade möjlighet att övervaka personuppgiftsbehandlingen.[149] Pseudonymisering definieras i artikel 4.5 GDPR som behandling av personuppgifter som inte längre kan tillskrivas en specifik registrerad utan att använda kompletterande information.[150] Pseudonymiserade personuppgifter omfattas alltjämt av GDPR.[151] I skäl 78 tydliggörs därtill att bevisbördan för att kraven uppfylls helt och hållet ligger på den som behandlar uppgifterna.[152] Den personuppgiftsansvarige kan bland annat visa att den uppfyller kraven genom att ansluta sig till en godkänd uppförandekod eller godkänd certifieringsmekanism.[153] Slutligen anges att den personuppgiftsansvarige eller personuppgiftsbiträdet ska vidta åtgärder för att anställda och annan personal som får tillgång till personuppgifter endast behandlar dessa på instruktion från den personuppgiftsansvarige.[154] Sådana instruktioner skulle till exempel kunna anges i de *back-to-back klausuler* som beskrevs ovan i avsnitt 2.3. Med hänsyn till att det ovan har konstaterats att informationshanteringen vid en due diligence är en personuppgiftsbehandling enligt GDPR måste dessa säkerhetsåtgärder vidtas i samband med en due diligence.[155]

GDPR medför vidare ett krav på att den personuppgiftsansvarige ska genomföra en konsekvensbedömning avseende behandlingen om en behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter med hänsyn till behandlingens art, omfattning, sammanhang och ändamål. Dessutom ska användande av ny teknik särskilt beaktas.[156] Att *ny teknik* ska beaktas vid avgörande om det krävs en konsekvensbedömning

[147] Art 32.1 GDPR.
[148] Artikel 29-gruppen, WP 250, s.6.
[149] Skäl 78 i GDPR.
[150] Art 4.5 GDPR.
[151] Skäl 26 i GDPR.
[152] Skäl 78 i GDPR.
[153] Art 32.3 GDPR.
[154] Art 32.4. GDPR.
[155] Se avsnitt 3.3.2.
[156] Art 35.1 GDPR.

medför att de arbetsmetoder som används vid en due diligence kan få betydelse för huruvida det krävs en konsekvensbedömning eller ej. Det torde till exempel föreligga en högre risk vid användning av ett virtuellt datarum jämfört med ett manuellt datarum. Vidare borde användning av AI-verktyg medföra en högre risk, vilket kommer behandlas närmare nedan i avsnitt 4.3.1. När behandling innebär en hög risk ska som framgår enligt ovan en konsekvensbedömning utföras. GDPR anger vidare tre situationer då det särskilt ska krävas en konsekvensbedömning; Vid en systematisk och omfattande bedömning av fysiska personer som grundar sig på automatisk behandling, innefattande profilering för vilken beslut som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer, vid behandling som omfattar känsliga personuppgifter i stor uträckning samt vid systematisk övervakning av en allmän plats i stor omfattning.[157] Konsekvensbedömningen innebär att den personuppgiftsansvarige, med utgångspunkt i en riskanalys, ska bedöma hur hög risk fysiska personers rättigheter och friheter utsätts för genom en planerad behandling. [158] Konsekvensbedömningen ska som huvudregel utföras före den planerade behandlingen påbörjas. Det är den personuppgiftsansvarige som ansvarar för att göra en självständig bedömning av den planerade behandlingen för att avgöra om det krävs en konsekvensbedömning i det enskilda fallet.[159]

3.4.3.2 Överföring av personuppgifter till andra personuppgiftsansvariga

Överföring av personuppgifter till annan personuppgiftsansvarig är i sig en aktivitet som innebär en personuppgiftsbehandling enligt GDPR.[160] Således måste den som överför personuppgifter se till att det finns en rättslig grund för den behandling som överföringen innebär samt att alla övriga principer i GDPR beaktas. Möjligheterna till att överföra personuppgifter är bland annat beroende av om det är en regelbunden, tillfällig eller enstaka överföring som avses. Vidare beror förutsättningarna för överföring på vad det är för typ av personuppgifter som ska överföras, mängden uppgifter samt hur överföringen ska ske rent tekniskt.[161] Som nämnts ovan ställs det särskilda krav på den rättsliga grunden om det är fråga om känsliga personuppgifter. Dessutom aktualiseras informationskraven i artikel 13 och 14 GDPR, vilka kommer att behandlas nedan. En överföring av personuppgifter från en

[157] Art 35.3 GDPR.
[158] Johansson(2018).
[159] Datainspektionen, *Förteckning över när en konsekvensbedömning ska göras.*
[160] Art 4.2 GDPR.
[161] Frydlinger(2018) s.231.

personuppgiftsansvarig till en annan personuppgiftsansvarig kan exempelvis aktualiseras i due diligence-sammanhang när en säljare överför personuppgifter till dess juridiska ombud.

I det fall att en överföring av personuppgifter sker till en organisation utanför EU gäller särskilda regler för överföringen. En överföring av personuppgifter till ett tredjeland kan till exempel bli aktuell vid ett företagsförvärv där köparen kommer från ett land utanför EU. Som tidigare nämnts föreligger det faktorer som talar för att förvärv där det finns en aktör som befinner sig utanför EU kommer att öka på den svenska marknaden för företagsförvärv. För att en överföring av personuppgifter till tredjeland ska tillåtas krävs förutom att övriga regler i GDPR ska vara uppfyllda att något av villkoren i förordningens kapitel fem är uppfyllt, således är huvudregeln att personuppgifter ej får överföras till tredjeland såvida inte överföringen är tillåten enligt någon av bestämmelserna i kapitel fem.[162] Först och främst får en överföring till tredjeland ske om kommissionen har beslutat att det aktuella tredjelandet säkerställer en adekvat skyddsnivå.[163] I detta sammanhang innehar USA en särställning genom den överenskommelse som fattades av EU och USA 2016 vilket utmynnade i beslutet om införandet av *Privacy Shield*.[164] Beslutet fattades på grundval av artikel 25.6 i det tidigare gällande dataskyddsdirektivet men är fortsatt gällande under GDPR.[165] Överenskommelsen innehåller principer om hur personuppgifter som överförs från EU till USA ska hanteras samt olika typer av översynsmekanismer som ska se till att principerna följs. Vidare innebär överenskommelsen att personuppgifter får överföras till amerikanska organisationer som har anslutit sig till Privacy Shield.[166] I avsaknad av ett kommissionsbeslut om adekvat skyddsnivå eller vid överföring till en amerikansk organisation som ej är ansluten till Privacy Shield kan överföringen ändå vara tillåten om den personuppgiftsansvarige eller personuppgiftsbiträdet vidtar lämpliga skyddsåtgärder i enlighet med artikel 46 GDPR, förutsatt att lagstadgade rättigheter och effektiva rättsmedel finns tillgängliga för de registrerade i det aktuella landet.[167] De lämpliga skyddsåtgärderna som kan vidtas kan delas upp i åtgärder som kräver och som inte kräver tillstånd från den behöriga tillsynsmyndigheten. Lämpliga skyddsåtgärder som inte kräver tillstånd kan vara bindande företagsbestämmelser som godkänts av tillsynsmyndigheten, standardiserade

[162] Art 44. GDPR.
[163] Art 45.1 GDPR.
[164] Kommissionens genomförandebeslut.
[165] Art 45.9 GDPR.
[166] Europeiska Kommissionen, *EU-US Data transfers*.
[167] Art 46. GDPR.

dataskyddsbestämmelser som godkänts av EU-kommissionen alternativt en godkänd uppförandekod eller godkänd certifiering. [168] Lämpliga skyddsåtgärder som kräver tillstånd kan istället vara egen utformade avtalsklausuler angående överföringen mellan den som överför personuppgifterna och mottagaren av personuppgifterna som befinner sig i ett tredjeland.[169] Innan en tillsynsmyndighet beslutar om tillstånd på grundval av sådana avtalsklausuler ska den begära ett yttrande från EDPB.[170] Om skyddet inte kan garanteras av lämpliga skyddsåtgärder kan överföringen likväl vara tillåten förutsatt att något av undantagen i artikel 49 GDPR är uppfyllt, exempelvis genom ett *uttryckligt* samtycke från de registrerade.[171]

3.4.3.3 Informationskraven i artikel 13 och 14

En av de grundläggande principerna i GDPR är principen om öppenhet och transparens.[172] Principen kommer bland annat till uttryck genom det informationskrav som gäller enligt artikel 13 och artikel 14 GDPR. I det fall personuppgifter som berör en registrerad person samlas in från de registrerade ska den personuppgiftsansvarige vid den tidpunkt personuppgifterna mottagits lämna information till de registrerade.[173] Kravet på information gäller även om personuppgifterna har mottagits på något annat sätt än från de registrerade.[174] Informationen ska i detta fall lämnas inom en rimlig period från det att personuppgifterna erhölls, dock senast inom en månad.[175] Dessutom aktualiseras informationskraven vid en överföring av personuppgifter till annan personuppgiftsansvarig.[176] GDPR anger ej i vilken form informationen ska lämnas till de registrerade. Däremot anges att den personuppgiftsansvarige har ett ansvar att vidta lämpliga åtgärder avseende informationsgivandet, vilket innebär att alla omständigheter om insamlandet och behandlingen ska beaktas när beslut tas om hur informationen ska lämnas till de registrerade.[177] Dessutom medför GDPR ett krav på att informationen ska vara koncis, klar

[168] Art 46.2 GDPR.
[169] Art 46.3 GDPR.
[170] Frydlinger m.fl.(2018) s. 240.
[171] Art 49.1 GDPR.
[172] Art 5.1 a GDPR.
[173] Art 13.1 GDPR.
[174] Art 14.1 GDPR.
[175] Art 14.3 a GDPR.
[176] Frydlinger m.fl.(2018) s. 233.
[177] Artikel 29-gruppen, WP 260, s. 13.

och tydlig, begriplig och i lättillgänglig form, med användning av klart och tydligt språk.[178] Kraven anses vara högt uppställda och kan i vissa sammanhang vara svåra att uppfylla.[179] Vilken information som ska lämnas till de registrerade anges i artikel 13 och 14 GDPR. Bland annat ska informationen innehålla ändamålen med den aktuella behandlingen samt den rättsliga grunden för behandlingen, de kategorier av personuppgifter som behandlingen gäller och om behandlingen grundar sig på artikel 6.1 f GDPR ska informationen innehålla den personuppgiftsansvariges eller tredjeparts berättigade intressen. Vidare ska informationen innefatta vilka kategorier av mottagare som ska ta del av personuppgifterna samt i förevarande fall om den personuppgiftsansvarige avser att överföra personuppgifterna till en mottagare i ett tredjeland. Dessutom ska lagringstiden för personuppgifterna anges och om det inte är möjligt vilka kriterier som används för att fastställa lagringstiden.[180]

Det finns dock undantag från ovanstående informationskrav, undantagen skiljer sig åt beroende på om personuppgifterna har samlats in direkt från de registrerade eller från annan. När personuppgifter samlas in direkt från de registrerade behöver information inte lämnas i det fall att de registrerade redan förfogar över informationen.[181] I det fall att personuppgifterna samlas in från någon annan än de registrerade gäller alltjämt undantaget som föreskriver att informationen inte behöver lämnas om de registrerade redan förfogar över informationen. Dessutom tillkommer följande undantag: det skulle vara omöjligt eller medföra oproportionell ansträngning att uppfylla informationskravet, erhållande eller utlämnande av uppgifter föreskrivs genom unionsrätten eller nationell lagstiftning som omfattar de registrerade och som fastställer lämpliga åtgärder för att skydda de registrerades berättigade intressen, eller om personuppgifterna måste förbli konfidentiella på grund av regler om tystnadsplikt enligt unionsrätt eller nationell rätt.[182] Vid en due diligence är det vanligast att informationen inhämtas på annat sätt än från de registrerade, exempelvis när en advokatbyrå får informationen från det säljande företaget. Därmed är det informationskravet i artikel 14 som för det mesta aktualiseras vid en due diligence.

[178] Art 12.1 GDPR.
[179] Frydlinger m.fl.(2018) s.168.
[180] Art 13.1, Art 14.1 och art 14.2 GDPR.
[181] Art 13.4. GDPR.
[182] Art 14.5 GDPR.

4. Due diligence och GDPR

4.1 Inledning

Som framgår av det ovan anförda innefattar informationshanteringen vid en due diligence hantering av personuppgifter så som de definieras i GDPR. Dessutom innebär informationshanteringen vid en due diligence personuppgiftsbehandling enligt GDPR. Det råder därmed inget tvivel om att GDPR medför konsekvenser för utformningen av due diligence-arbetet. Nedan följer en analys över områden i due diligence-arbetet som påverkas samt hur de påverkas. Dessutom kommer kapitlet att diskutera hur påverkan av GDPR kan hanteras inom ramen för en due diligence.

4.2 Rättslig grund

4.2.1 Rättslig grund för att lägga in personuppgifter i datarum

Vid en due diligence sker det i regel ingen insamling av personuppgifter. Däremot innebär införandet av personuppgifter i ett datarum en personuppgiftsbehandling.[183] Följaktligen krävs det rättslig grund för att föra in personuppgifterna i datarummet för att säkerställa att reglerna i GDPR efterlevs.

En första utgångspunkt är att den personuppgiftsansvarige har rättslig grund för att behandla personuppgifter i det fall att de registrerade har samtyckt till behandlingen. För att ett samtycke ska utgöra rättslig grund krävs att de krav som redogavs för i avsnitt 3.4.2 är uppfyllda. Därmed måste samtycket bland annat vara specifikt för den aktuella due diligence-processen. I det fall den personuppgiftsansvarige inte har något samtycke från de registrerade krävs att någon av de andra grunderna i artikel 6 GDPR är tillämpliga.

En grund som skulle kunna vara tillämplig för personuppgiftsbehandling vid en due diligence är grunden i artikel 6.1 f GDPR. Bestämmelsen är tillämplig om behandlingen är *nödvändig* för ändamål som avser den personuppgiftsansvariges eller tredjeparts *berättigade intressen* om inte de registrerades intressen eller grundläggande rättigheter *väger tyngre* och kräver

[183] Se avsnitt 3.3.2.

skydd av personuppgifter. Att utföra en fullständig due diligence utan att behandla några personuppgifter torde inte vara möjligt. För att utföra en fullständig due diligence krävs att målbolagets dokumentation gås igenom grundligt vilket förmodligen inte hade varit möjligt om personuppgifter undantas från undersökningen. Således skulle det kunna argumenteras för att nödvändighetsrekvisitet i ovanstående bestämmelse är uppfyllt. Huruvida en behandling är nödvändig eller ej enligt GDPR beror dock på omständigheter i varje enskilt fall vilket medför att det inte går att dra någon generell slutsats i frågan.

När det kommer till intresseavvägningen kan bedömningen som tidigare nämnts delas upp i fyra olika moment:

1. *Identifiera aktörer*

De relevanta aktörerna torde vanligtvis vara personuppgiftsansvarig i form av säljare och köpare med respektive ombud samt de registrerade. Aktörernas intressen är i sammanhanget att genomföra ett företagsförvärv alternativt behandla personuppgifter vid utförande av uppdrag för sin klient respektive skydd för de registrerades personuppgifter.

2. *Identifiera berättigade intressen*

Vid avgörande om det föreligger ett berättigat intresse ska det bland annat göras en bedömning över huruvida det aktuella intresset är lagenligt, tydligt och reellt. Intresset vid en due diligence kan som nämnts ovan vara att genomföra ett företagsförvärv eller behandla personuppgifter vid utförande av uppdrag för klient. Det finns ingenting som tyder på att ovanstående intressen skulle vara lagstridiga. Vidare torde nämnda intressen vara tillräckligt tydligt formulerade för att genomföra en intresseavvägning med hänsyn till att intressena är specifika och att det därigenom är möjligt att väga intressena mot varandra i en intresseavvägning. Slutligen är intressena nuvarande och reella intressen förutsatt att intresseavvägningen utförs när ett företagsförvärv ligger för handen eftersom det i sådant fall varken är framtida eller hypotetiskt. I sammanhanget bör det dock noteras att ovanstående bedömningar är av ett generellt slag och att det därmed kan föreligga omständigheter i samband med en due diligence som inte har tagits hänsyn till. Det skulle exempelvis kunna uppstå en situation när personuppgifter behandlas i en *vendor due diligence* utan att det är klart att ett företagsförvärv ska genomföras vilket i sådant fall torde innebära att intresset är framtida och hypotetiskt och således ej ett berättigat intresse.

3. *Identifiera registrerades intressen eller rättigheter*

Mängden personuppgifter som behandlas, vad det är för typ av personuppgifter samt vad personuppgifterna ska användas till är alla faktorer som varierar i olika due diligence-förfaranden. Därmed går det inte att göra en generell bedömning avseende dessa faktorer. Däremot kan det nämnas att om det exempelvis är en stor mängd personuppgifter som behandlas eller om det är känsliga personuppgifter som behandlas förutsätts ett starkare skydd för de registrerades personuppgifter. Huruvida de registrerade skulle kunna förvänta sig att en personuppgiftsbehandling i form av informationshantering i samband med en due diligence skulle kunna komma att ske vid inhämtandet av personuppgifterna beror på omständigheterna i varje enskilt fall och det är därför inte möjligt att dra någon generell slutsats i frågan. Däremot torde det åtminstone inte vara orimligt att de skulle kunna förvänta sig en personuppgiftsbehandling av det aktuella slaget.

4. Övergripande avvägning

Den övergripande helhetsbedömningen beror precis som flera av de ovan nämnda bedömningarna på omständigheter i det enskilda fallet. Det kan dock konstateras att den personuppgiftsansvarige kan vidta åtgärder för att öka sannolikheten för att intresseavvägningen ska leda till rättslig grund. Sådana åtgärder kan exempelvis vara: tekniska och organisatoriska åtgärder som begränsar den personuppgiftsansvariges möjligheter att använda personuppgifterna, omfattande användning av anonymiseringstekniker, åtgärder för inbyggt dataskydd, ökad transparens gentemot de registrerade avseende vilka personuppgifter som används och hur.[184] Omständigheter som kan göra att de registrerades intressen och rättigheter väger tyngre kan som tidigare nämnts exempelvis vara att personuppgiftsbehandlingen innefattar en omfattande mängd personuppgifter.

Som framgår enligt ovan beror intresseavvägningen på flera omständigheter som varierar i varje enskilt fall. Det går således inte att fastställa att artikel 6.1 f GDPR utgör rättslig grund för personuppgiftsbehandling i samband med informationshanteringen vid en due diligence. Däremot går det inte heller att fastställa att artikel 6.1 f GDPR inte utgör rättslig grund för en

[184] Artikel 29-gruppen, WP 217, s. 42.

sådan behandling vilket leder till slutsatsen att det beror på omständigheterna i varje enskilt fall.

En annan grund som skulle kunna diskuteras är avtalsgrunden i artikel 6.1 b GDPR. För att den ska vara tillämplig krävs att de registrerade själva är part i avtalet. Vilket medför att ett avtal mellan en advokatbyrå och en annan juridisk person, till exempel ett uppdragsavtal för utförande av due diligence, ej innebär att advokatbyrån får behandla personuppgifter om anställda hos den juridiska personen mot bakgrund av ovanstående grund eftersom de registrerade i sådant fall inte är parter i avtalet. Däremot förekommer det avtal där de registrerade är parter i den dokumentation som återfinns vid informationshanteringen i en due diligence, exempelvis i form av anställningsavtal. För att ovanstående grund ska vara tillämplig krävs dock att åtgärden i fråga är nödvändig för att *fullgöra* ett avtal. Att behandla personuppgifter i syfte att utföra en due diligence borde inte anses nödvändigt för att till exempel fullgöra ett anställningsavtal. Advokatsamfundet anger fakturering, klientregistrering och förandet av klientkonton som exempel på åtgärder som kan omfattas av avtalsgrunden.[185] Således torde inte ovanstående grund kunna användas för att rättfärdiga behandling av personuppgifter i samband med en due diligence.

I det fall att det rör sig om känsliga personuppgifter som ska föras in i datarummet är behandlingen förbjuden såvida inte något av undantagen är uppfyllda.[186] Det enda undantaget som skulle kunna vara tillämpligt vid en due diligence är att de registrerade har samtyckt till behandlingen, ett sådant samtycke måste förutom att uppfylla de övriga kraven för ett giltigt samtycke vara *uttryckligt*.[187]

4.2.2 Handlingsförslag för säkerställande av regelefterlevnad

Vid en due diligence förekommer personuppgifter som rör många olika personer, i synnerhet vid större transaktioner. Det är inte särskilt sannolikt att ett företag har samtycke från alla berörda personer när personuppgifterna ska föras in i datarummet. Arbetet vid en due diligence sker i de flesta fall under en relativt stor tidspress och med hänsyn till att inhämtandet av samtycke från alla berörda personer är en tidskrävande process är det inget

[185] Advokatsamfundet(2018) s.30.
[186] Se avsnitt 3.3.1.
[187] Se avsnitt 3.3.1.

bra alternativ. Dessutom innefattar de flesta företagsförvärv moment av hemlighetsmakeri vilket medför att företagen inte vill meddela alla personer om att ett företagsförvärv ligger för handen, vilket hade varit nödvändigt för att inhämta samtycke från de berörda personerna. Följaktligen är det med största sannolikhet svårt för den personuppgiftsansvarige att, vid en due diligence, förlita sig på samtycke som rättslig grund för behandling av personuppgifterna. Dessutom kan ett samtycke när som helst återkallas vilket skulle medföra en osäkerhet för en personuppgiftsansvarig som förlitar sig på samtycke som rättslig grund.

Med hänsyn till den ovanstående problematiken kring att förlita sig på samtycke som rättslig grund är den rättsliga grunden som anges i artikel 6.1 f GDPR ett bättre alternativ. Som framgår enligt ovan beror dess tillämplighet på omständigheter i varje enskilt fall och olika omständigheter kan få intresseavvägningen att väga åt olika håll. I syfte att öka sannolikheten för att en sådan intresseavvägning leder till rättslig grund finns det flera åtgärder som den personuppgiftsansvarige kan vidta eftersom vidtagande av ytterligare åtgärder är något som ska beaktas vid intresseavvägningen. En första åtgärd som kan vidtas är att endast lägga in de personuppgifter som är absolut nödvändiga för utförandet av en due diligence, alltså en begränsning av antalet personuppgifter som förs in i datarummet. Det bör dock noteras att det innebär en risk för säljaren att begränsa materialet som tillgängliggörs för köparen. Omfattningen av köparens undersökningsplikt blir, som tidigare nämnts, mindre i det fall att materialet begränsas.[188] Således ökar möjligheten för köparen att rikta rättsliga anspråk mot säljaren om materialet som tillgängliggörs begränsas. Däremot bör det tilläggas att om det kan konstateras att vissa personuppgifter inte medför någon risk alternativt liten risk för att leda till brister i målbolaget torde dessa kunna utelämnas i syfte att säkerställa regelefterlevnad med GDPR. En annan åtgärd som kan reducera antalet införda personuppgifter är att sammanfatta de avtal som liknar varandra, exempelvis genom att endast ladda upp ett anställningsavtal för en viss grupp anställda istället för att ladda upp alla anställningsavtal då de ändå har liknande innehåll. Vidare kan säkerhetsåtgärder som exempelvis pseudonymisering och upprättande av ett separat datarum för HR-avdelningen vidtas, vilka kommer behandlas närmare under avsnitt 4.5. Sådana säkerhetsåtgärder bör påverka intresseavvägningen i artikel 6.1 f i positiv riktning för den personuppgiftsansvarige.

[188] Se avsnitt 2.2.

Vad gäller känsliga personuppgifter har det konstaterats att de endast får föras in i datarummet om de registrerade har givit sitt uttryckliga samtycke. Ett alternativ i avsaknad av ett sådant samtycke skulle kunna vara att anonymisera den information som är av sådant slag att den omfattas av artikel 9.1 och därmed är att se som känsliga personuppgifter. Personuppgifter som har anonymiserats på ett sådant sätt att de registrerade inte längre är identifierbara omfattas inte av GDPR.[189] För att anonymisera personuppgifterna krävs därför att det inte finns några uppgifter som överhuvudtaget går att koppla till de registrerade. Anonymisering av personuppgifter kan uppnås genom flera olika tekniker som i regel faller inom antingen *randomisering* eller *generalisering*.[190]

4.3 Säkerhetsåtgärder

4.3.1 Säkerhetsåtgärder och due diligence

Informationshanteringen vid en due diligence innebär som tidigare nämnts en personuppgiftsbehandling. Därmed måste den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder vid det due diligence-arbete som innefattar behandling av personuppgifter.[191]

GDPR medför även ett krav på att en konsekvensbedömning ska utföras vid behandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter med hänsyn till behandlingens art, omfattning, sammanhang och ändamål med särskilt beaktande av om ny teknik används.[192] Således uppkommer frågan om behandlingen vid en due diligence är av sådan art att GDPR föreskriver att en konsekvensbedömning måste utföras före behandlingen. GDPR anger tre situationer när en konsekvensbedömning ska krävas, ingen av de situationer som anges omfattar personuppgiftsbehandlingen vid en due diligence.[193] De situationer som anges är dock ingen uttömmande förteckning varför andra typer av behandlingar ändå kan kräva en konsekvensbedömning.[194] Med hänsyn till att behandlingen innebär att

[189] Skäl 26 i GDPR.
[190] Voigt och von dem Bussche(2017) s.13.
[191] Se avsnitt 3.4.2.
[192] Se avsnitt 3.4.2.
[193] Se avsnitt 3.4.2.
[194] Art 29-gruppen, WP248, *s.10.*

personuppgifterna införs i ett datarum som endast ett begränsat antal har tillgång till torde det inte föreligga en hög risk för fysiska personers rättigheter och friheter. I det här sammanhanget är användning av AI vid en due diligence intressant att ta upp. Flertalet svenska affärsjuridiska byråer har börjat implementera olika system för AI och många i branschen tror att det kommer bli allt mer vanligt.[195] Due diligence är vidare ett område inom juridiken som är ett väl lämpat användningsområde för AI då AI-verktygen kan samla in och hantera stora mängder information. Kira Systems är en av de ledande leverantörerna på marknaden för AI-verktyg. De levererar ett AI-verktyg som genom maskininlärning[196] kan automatisera arbetet vid en due diligence. Automatiseringen går till på så sätt att verktyget analyserar och sammanfattar den dokumentation som finns tillgänglig i datarummet för att sedan uppmärksamma jurister på risker i dokumentationen. Verktyget fungerar genom att en jurist väljer vilken typ av information som ska hittas, exempelvis alla *change of control-klausule*r, och sedan kan verktyget hitta alla sådana klausuler i de avtal som det söker igenom.[197] Med hänsyn till att AI är en ny teknologi torde det anses sannolikt att AI-behandling av personuppgifter leder till hög risk för fysiska personers rättigheter och friheter. Därmed krävs det med största sannolikt en konsekvensbedömning i de fall då AI används vid informationshanteringen i samband med en due diligence. Vidare menar Advokatsamfundet att AI-lösningar kan motivera en konsekvensbedömning.[198] Det kan även tilläggas att en konsekvensbedömning, enligt artikel 29-gruppen, bör utföras i de situationer då det är osäkert huruvida en konsekvensbedömning är nödvändig eller ej med hänsyn till att det kan vara ett användbart redskap för att hjälpa den personuppgiftsansvarige att följa reglerna i GDPR. [199]

4.3.2 Handlingsförslag för säkerställande av regelefterlevnad

I skälen till GDPR anges ett antal förslag på åtgärder som den personuppgiftsansvarige kan vidta för att uppfylla förordningens krav på säkerhet. Minimering av uppgiftsbehandlingen och pseudonymisering av personuppgifterna är två av de förslag som anges.[200] Således finns det ytterligare anledning för den personuppgiftsansvarige som för in personuppgifterna i datarummet att pseudonymisera dessa personuppgifter innan de förs in i datarummet. Som

[195] Persson och Knutsson(2017) s.38-ff.
[196] *Maskininlärning* är en teknik som möjliggör att datorer har förmåga att förbättra sin prestanda genom att utsättas för data utan att följa programmerade instruktioner.
[197] Kira Systems.
[198] Advokatsamfundet (2018) s.45.
[199] Art 29-gruppen, WP248, *s.9.*
[200] Skäl 78 till GDPR.

tidigare nämnts innebär pseudonymisering att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan kompletterande information men att sådana personuppgifter fortfarande omfattas av GDPR.[201] Rent praktiskt finns det olika sätt att pseudonymisera personuppgifter. En metod är den så kallade *substitutionsmetoden* vilken innebär att information om de registrerade modifieras samtidigt som det kvarstår en koppling mellan informationen och de registrerade, exempelvis kan de registrerades namn modifieras medan det kvarstår en koppling mellan andra uppgifter som till exempel adress och kundnummer. Ytterligare en teknik för pseudonymisering är *maskning* vilket innebär att en del av informationen om de registrerade göms, exempelvis genom att de fyra sista siffrorna i ett personnummer ersätts med tecken.[202] Dessutom föreligger det anledning att minimera uppgiftsbehandlingen genom att behandla så lite personuppgifter som möjligt. Dessa två säkerhetsåtgärder kan som nämnts i avsnitt 4.2.3. även användas för att tillförsäkra att det finns rättslig grund för behandlingen.

En annan åtgärd som den personuppgiftsansvarige skulle kunna vidta är att upprätta ett separat datarum för företagets HR-funktion som endast ett visst antal personer får tillgång till exempelvis endast en jurist från arbetsrättsgruppen. HR-funktionen är den del av företaget där det finns flest personuppgifter. Åtgärden innebär en ökad säkerhet för de registrerades personuppgifter med hänsyn till att risken för obehörig åtkomst reduceras genom att antalet personer som får tillgång till personuppgifterna begränsas.

Ytterligare en aspekt som är viktig i det här avseendet är att den personuppgiftsansvarige bör upprätta utförliga och välgenomtänkta sekretessavtal som ingås med de inblandade aktörerna före utförandet av en due diligence. Som tidigare nämnts råder det avtalsfrihet rörande sekretessavtal och parterna kan därmed utforma sekretessavtalen på ett sätt som de finner lämpligt.[203] Följaktligen finns det möjlighet för den personuppgiftsansvarige att, i de sekretessavtal som ingås med de inblandade aktörerna, införa bestämmelser avseende personuppgiftsbehandlingen vid en due diligence. Bestämmelser som skulle kunna vara relevanta att föra in i ett sekretessavtal är exempelvis skyldighet att återlämna eller förstöra information i det fall att förhandlingarna strandar, endast använda informationen för dess syfte, hålla informationen inom den relevanta jurisdiktionen samt vidtagande av lämpliga

[201] Art 4.5 GDPR och Skäl 26 i GDPR.
[202] 24solutions, *Pseudonymisering och anonymisering av persondata- vad är skillnaden?*
[203] Se avsnitt 2.3.

säkerhetsåtgärder. Med tydliga bestämmelser om informationshanteringen av personuppgifter ökar säkerheten för de registrerades rättigheter.

Vad gäller konsekvensbedömningen är det som nämnts ovan den personuppgiftsansvarige som ska göra en självständig bedömning över huruvida en konsekvensbedömning är nödvändig. Med hänsyn till artikel 29-gruppens rekommendation om att den personuppgiftsansvarige bör utföra en konsekvensbedömning i osäkra fall torde det föreligga anledning för den personuppgiftsansvarige att utföra en konsekvensbedömning såvida denne inte är helt säker på att det inte krävs. Vidare bör en konsekvensbedömning alltid utföras i de fall då den personuppgiftsansvarige, i personuppgiftsbehandlingen, använder sig av ny teknik som till exempel AI.

4.4 Överföring till annan personuppgiftsansvarig

4.4.1 Överföring inom EU

En överföring av personuppgifter innebär som tidigare nämnts en personuppgiftsbehandling vilket innebär att det krävs rättslig grund för att en överföring av personuppgifter ska vara förenlig med GDPR. I avsnitt 4.2. redogjordes för huruvida den personuppgiftsansvarige har rättslig grund för att föra in personuppgifter i ett datarum. Även i det här fallet är det intresseavvägningen i artikel 6.1 f som skulle kunna vara den rättsliga grunden för överföringen. Med det sagt är det dock viktigt att observera att det blir fråga om en ny intresseavvägning.

4.4.2 Överföring utanför EU

En överföring av personuppgifter till en personuppgiftsansvarig utanför EU kan till exempel bli aktuellt om köparen i företagsförvärvet är ett företag som befinner sig utanför EU. Med hänsyn till det ovan nämnda intresset från asiatiska och amerikanska aktörer samt med hänsyn till en potentiell ”no-deal” Brexit föreligger det anledning att anta att företagsförvärven, där det finns en inblandad aktör utanför EU, kommer att öka varför frågan om överföring till personuppgiftsansvarig utanför EU är högst relevant.

En överföring till ett tredjeland är som ovan nämnts endast tillåten om något av villkoren i förordningens 5:e kapitel är uppfyllt. För det första är en överföring av ovan nämnda slag tillåten om den sker till ett land som kommissionen har beslutat har en adekvat skyddsnivå, och när det gäller USA företag som är anslutna till Privacy Shield.[204] Villkoret föranleder inte några komplexa frågeställningar för en personuppgiftsansvarig som i en due diligence ämnar överföra personuppgifter till ett tredjeland. Däremot är det relativt få länder som har tillmätts en sådan adekvat skyddsnivå varför det i många fall inte kommer vara möjligt att förlita sig på detta villkor.[205] I de fall den personuppgiftsansvarige eller personuppgiftsbiträdet inte kan förlita sig på ovanstående villkor kan den istället förlita sig på villkoren i artikel 46 GDPR. Bestämmelsen föreskriver att tredjelandsöverföringen är tillåten om den personuppgiftsansvarige vidtagit lämpliga skyddsåtgärder samt förutsatt att lagstadgade rättigheter och effektiva rättsmedel för de registrerade finns tillgängliga.[206]

Vid det fall att inget av ovanstående villkor är uppfyllt får en överföring ändå äga rum om något av villkoren i artikel 49 GDPR ligger för handen. För det första är en överföring till tredjeland tillåten om de registrerade lämnat sitt *uttryckliga* samtycke. Kravet på samtycke innebär att de allmänna kraven som redogjorts för i avsnitt 3.4.2. måste vara uppfyllda. Dessutom finns särskilda krav på samtycket i det här sammanhanget. För att samtycket ska vara giltigt enligt artikel 49 GDPR krävs först och främst att det har getts specifikt för den aktuella överföringen. Vidare krävs, för att samtycket ska vara giltigt, att de registrerade informeras om de särskilda risker som överföringen innebär.[207] De övriga villkoren torde inte vara tillämpliga vid överföring till tredjeland i samband med en due diligence varför samtycke står som det enda möjliga alternativet. Utnyttjande av villkoren i artikel 49 GDPR får dock aldrig resultera i en situation där de registrerades grundläggande rättigheter kränks.[208] Därmed bör villkoren i artikel 49 GDPR endast utnyttjas först efter att mekanismerna i artikel 45 och 46 har utretts.[209] Villkoren i artikel 49 GDPR är undantag från den allmänna principen om att överföring till tredjeland endast får ske om en adekvat skyddsnivå tillhandahålls i landet eller om lämpliga skyddsåtgärder vidtagits.[210] Med hänsyn till att villkoren är undantag från en allmän princip och i enlighet med EU-rättens inneboende

[204] Se avsnitt 3.4.3.
[205] Europeiska Kommissionen, *Adequacy decisions.*
[206] Se avsnitt 3.4.3.
[207] EDPB, Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679. s.7.
[208] Art 29-gruppen, WP 114, s.9.
[209] EDPB, Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679 s.4.
[210] Skäl 114. GDPR.

principer krävs att dessa villkor tolkas restriktivt, för att undantaget inte ska bli till regel.[211] EDPB menar att samtycke förmodligen inte är en praktiskt användbar långsiktig lösning för överföringar av personuppgifter till tredjeland med hänsyn till kombinationen av de höga kraven för undantag tillsammans med att de registrerades samtycke när som helst kan återkallas.[212] Med hänsyn till ovanstående resonemang kommer det vara av yttersta vikt för en personuppgiftsansvarig, som i samband med en due diligence ska överföra personuppgifter till tredjeland, att tillförsäkra sig om att villkoren i artikel 45 eller 46 är uppfyllda.

4.4.3 Handlingsförslag för säkerställande av regelefterlevnad

Vid en överföring av personuppgifter, oavsett om överföringen sker inom eller utanför EU, är det lämpligt att fastslå vilka principer som gäller för överföringen i ett datadelningsavtal, genom ett sådant avtal tydliggörs överföringens förutsättningar samt eventuella villkor som den överförande organisationen har satt upp för överföringen.[213]

När det kommer till villkoret i artikel 45 finns det inte särskilt mycket för den överförande aktören att göra förutom att vara uppmärksam på om överföringen sker till ett land med en adekvat skyddsnivå eller ej.

Vad gäller uppfyllande av villkoren i artikel 46 GDPR finns det som tidigare nämnts flera alternativ för den personuppgiftsansvariga, alltså alternativ för vidtagande av lämpliga skyddsåtgärder. Alternativen reduceras dock när det kommer till möjliga alternativ att vidta vid en överföring av personuppgifter i samband med en due diligence. En första lämplig skyddsåtgärd som kan vidtas i samband med en due diligence är ingående av avtal som innehåller standardavtalsklausuler vilka har godkänts av EU-kommissionen. I det fall att en personuppgiftsansvarig ingår avtal som innehåller sådana standardavtalsklausuler med någon som befinner sig utanför EU är det tillåtet att överföra personuppgifter till denne.[214] Det är viktigt att notera att sådana klausuler inte får ändras, såvida det inte är nödvändigt och rör affärsrelaterade frågor och då endast om de inte strider mot någon standardavtalsklausul.[215] Standardavtalsklausulerna innehåller skyldigheter för den personuppgiftsansvarige som

[211] Art 29-gruppen, WP 114, s.7.
[212] EDPB, Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679 s.8.
[213] Frydlinger(2018) s.232.
[214] Art 46.2 c GDPR.
[215] Datainspektionen, *Hur vidtar vi lämpliga skyddsåtgärder?*

överför personuppgifterna samt för den som tar emot personuppgifterna. Klausulerna innefattar dessutom reglering av andra frågor avseende överföringen, som till exempel de registrerades rättigheter och hur tvister med anledning av avtalet ska lösas.[216] Standardklausuler av ovan nämnda slag skulle exempelvis kunna biläggas som bilaga till ett sådant datadelningsavtal som nämndes ovan. Ett annat alternativ är att grunda överföringen på avtalsklausuler som parterna utformar på egen hand. En överföring till tredjeland kan vara tillåten om det finns egen utformade avtalsklausuler som reglerar överföringen mellan den som överför personuppgifterna och mottagaren av dessa. För att sådana avtalsklausuler ska kunna ligga till grund för en överföring krävs dock tillstånd från den behöriga tillsynsmyndigheten,[217] vilket i Sveriges fall är Datainspektionen. Likt standardavtalsklausulerna skulle sådana egenutformade avtalsklausuler kunna biläggas som bilaga till ett datadelningsavtal.

Beroende på omständigheterna i det enskilda fallet kan det ena alternativet vara mer lämpligt än det andra. Standardavtalsklausuler är enligt min mening det mest optimala alternativet, förutsatt att båda parter är tillfreds med innehållet i dessa klausuler, eftersom det i sådant fall inte krävs något tillstånd från Datainspektionen. Däremot, om någon av parterna inte kan tänka sig att acceptera innehållet i sådana klausuler är det istället mer lämpligt att söka tillstånd hos Datainspektionen och utforma egna avtalsklausuler rörande överföringen som tillgodoser parternas intressen. Med hänsyn till att de egenutformade avtalsklausulerna förutsätter tillstånd samt att innehållet i standardavtalsklausulerna är av sådant slag att de torde accepteras av många personuppgiftsansvariga förefaller det vara relativt ovanligt att egenutformade avtalsklausuler används som lämplig skyddsåtgärd.

4.5 Informationskraven i artikel 13 och 14 GDPR

4.5.1 Informationskraven vid en due diligence

Informationshanteringen av personuppgifter vid en due diligence sker i regel avseende personuppgifter som redan har samlats in från de registrerade. Därmed är det informationskravet i artikel 14 GDPR som är mest relevant, personuppgifter inhämtade från annan än de registrerade. Således är den personuppgiftsansvarige före utförandet av det due

[216] Frydlinger m.fl.(2018) s. 242.
[217] Art 46.3 a. GDPR.

diligence-arbete som innebär överföring av personuppgifter skyldig att lämna information till de registrerade som berörs.[218] Som tidigare nämnts finns det dock undantag till ovanstående informationskrav.[219] Ett av undantagen föreligger om de registrerade redan förfogar över informationen. Ytterligare undantag som skulle kunna vara tillämpligt för en personuppgiftsansvarig vid en due diligence är att det skulle vara omöjligt eller medföra en oproportionell ansträngning att förse de registrerade med den nödvändiga informationen. För att förlita sig på undantaget om att det är *omöjligt* att utge information måste den personuppgiftsansvarige kunna visa de faktorer som faktiskt förhindrar denne från att förse de registrerade med informationen. Enligt artikel 29-gruppen är det ett begränsat antal situationer som omfattas av det här undantaget.[220] Vid utförandet av en due diligence finns det förmodligen inga faktorer som faktiskt kan förhindra den personuppgiftsansvarige från att förse de registrerade med information varför det med största sannolikhet ej kan bli tillämpligt i samband med informationshanteringen vid en due diligence. När det kommer till undantaget rörande *oproportionell ansträngning* bör det noteras att det särskilt riktar sig till behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Därmed bör undantaget, enligt artikel 29-gruppen, inte användas rutinmässigt av personuppgiftsansvariga som inte arbetar med sådan behandling.[221] Personuppgiftsbehandlingen vid en due diligence innefattar inte något av ovanstående ändamål och således torde inte heller detta undantag kunna användas vid utförandet av en due diligence.

Därmed kan det konstateras att det visserligen finns undantag från informationskravet som skulle kunna vara tillämpliga för en personuppgiftsansvarig vid en due diligence. Undantagen ska dock, som huvudregel, tillämpas restriktivt.[222] Dessutom torde inte undantagen avseende *omöjlighet* och *oproportionell ansträngning* vara tillämpliga för informationshanteringen i samband med en due diligence.

[218] Se avsnitt 3.4.3.
[219] Se avsnitt 3.4.3.
[220] Artikel 29-gruppen, WP 260, s.29.
[221] Artikel 29-gruppen, WP 260, s.30.
[222] Ibid. s.28.

4.5.2 Handlingsförslag för säkerställande regelefterlevnad

Att utge information om personuppgiftsbehandlingen vid en due diligence till alla registrerade skulle innebära en mycket tidskrävande process. Dessutom vill företagen, som nämnts ovan, i de allra flesta fall hålla ett företagsförvärv hemligt varför utgivande av information till alla registrerade inte är ett önskvärt alternativ.

För att den personuppgiftsansvarige inte ska behöva utge information krävs att något av undantagen är uppfyllda. Det har ovan konstaterats att undantagen som avser omöjlighet och oproportionell ansträngning kan vara svåra att uppfylla och att förlita sig på något av dessa undantag skulle därmed kunna vara en säkerhetsrisk med hänsyn till att det skulle kunna leda till överträdelse av reglerna i GDPR. Det mest optimala alternativet för den personuppgiftsansvarige är istället, enligt min mening, att försöka tillförsäkra att de registrerade redan förfogar över informationen. En åtgärd för att tillförsäkra att de registrerade förfogar över informationen är att lägga in en skrivelse i företagets personuppgiftspolicy vilken föreskriver den nödvändiga informationen som krävs i samband med överföring av personuppgifter i samband med ett företagsförvärv.

Nedan följer ett antal utdrag hur olika företags personuppgiftspolicys avseende personuppgiftsbehandling i samband med ett företagsförvärv med efterföljande kommentarer.

Företag: Expedia AB
Skrivelse: *I samband med en företagstransaktion, såsom vid försäljning av ett dotterbolag eller en verksamhet, fusion, konsolidering, försäljning av egendom eller vid den osannolika händelsen att vårt företag går i konkurs. Vid eventuellt företagsförvärv informerar vi köparen om att denna endast får använda dina personuppgifter för de ändamål som beskrivs i denna Personuppgiftspolicy.*[223]

Företag: Dplay
***Skrivelse*:**
Fusion eller förvärv*: Vi kan komma att lämna ut dina personuppgifter om Dplay om vi förvärvas av, eller fusioneras med, ett annat företag. Skulle vi involveras i en fusion, ett förvärv, eller en försäljning av samtliga eller en del av våra tillgångar så kommer du att meddelas i efterhand via mejl och/eller genom tydligt meddelande i våra Tjänster kring förändringar i äganderätten eller användningen av dina personuppgifter, samt eventuella valmöjligheter du har beträffande dina personuppgifter.*[224]

Företag: Ramirent AB
Skrivelse:
Vid fusion, förvärv eller försäljning*: För det fall Ramirent blir föremål för en fusion, ett förvärv eller en försäljning av alla eller delar av våra tillgångar kan dina personuppgifter delas med en potentiell köpare och*

[223] Expedia AB.
[224] Dplay AB.

om tillgångar eller Ramirent i sin helhet förvärvas av en tredje part kan personuppgifter om våra kunder komma att delas med sådan tredje part.[225]

***Företag**:* Essity AB
***Skrivelse**: I enlighet med tillämplig personuppgiftslagstiftning kan Essity komma att överföra personuppgifter till tillsynsmyndigheter, andra offentliga organ, juridiska rådgivare, externa konsulter och samarbetspartners. I händelse av en sammanslagning eller förvärv av företag kan personuppgifter komma att överföras till tredje parter som är involverade i sammanslagningen eller förvärvet.*[226]

Företag: Visma AB
***Skrivelse*:**
Sammanslagningar och förvärv
I samband med sammanslagningar, förvärv eller avyttring av hela eller delar av Vismas verksamhet får den förvärvande enheten samt dess konsulter tillgång till uppgifter som berörd enhet/berörda enheter inom Visma har hanterat, vilket kan omfatta personuppgifter. I dessa fall ingår externa parter ett sekretessavtal med Visma.[227]

Kommentar: Som framgår av ovanstående skrivelser är de bristfälliga i flera avseenden i förhållande till informationskraven i GDPR. Bland annat saknar samtliga skrivelser den rättsliga grunden för behandlingen, vilka kategorier av personuppgifter som behandlingen gäller samt lagringstiden för personuppgifterna. Således kan det konstateras att ingen av ovanstående skrivelser uppfyller undantaget från informationskraven som avser att de registrerade redan förfogar över informationen.

Företag: Sagax AB

Skrivelse:
Vid företagsförvärv

Vi kan komma att använda dina personuppgifter vid ett företagsförvärv eller vid omstrukturering av Sagax. Vi grundar denna behandling på en intresseavvägning, eftersom vi bedömer att vårt intresse av att möjliggöra en förvärvs- eller omstruktureringsprocess överväger ditt intresse av skydd för dina personuppgifter. Det förutsätter dock att det övertagande bolaget bedriver liknande verksamhet som Sagax. Om Sagax upphör att existera, till exempel genom en fusion, likvidation eller konkurs, kommer dina personuppgifter raderas så länge de inte behöver sparas för att uppfylla lagkrav.

Om Sagax förvärvas av ett övertagande bolag eller delas upp i samband med en omstrukturering kommer dina personuppgifter att fortsätta sparas och användas av det övertagande bolaget enligt villkoren i denna integritetspolicy, om du inte får annan information i samband med överlåtelsen. Detsamma gäller om Sagax säljer en fastighet som du i egenskap av hyresgäst, leverantör eller samarbetspartner har anknytning till.[228]

***Kommentar**:* I ovanstående skrivelse saknas vilka kategorier av personuppgifter som behandlingen avser. Det finns inte heller någon information om vilka kategorier av mottagare

[225] Ramirent AB.
[226] Essity AB.
[227] Visma AB.
[228] Sagax AB.

som ska ta del av personuppgifterna. Därmed uppfyller inte heller ovanstående skrivelse undantaget från informationskraven.

Företag: Edenred Sweden AB

Skrivelse:

SYFTE*:*

Administration i samband med företagsförvärv eller omstrukturering av Edenred etc.

PERSONUPPGIFTER*:*

Kontaktuppgifter såsom namn, telefonnummer och e-postadress

Order- och betalningsuppgifter såsom köp- och transaktionshistorik.

Arbetsrelaterad information såsom företagsnamn och organisationsnummer

VAD VI GÖR:

Om Edenred ska omstruktureras, t.ex. delas upp i flera olika verksamheter, eller om en utomstående part önskar förvärva Edenred eller vår kunddatabas kommer Edenred att lämna ut dina och andra kunders personuppgifter till det övertagande bolaget. Det bolaget kommer i sådana fall att fortsätta använda dina personuppgifter för samma syften som de vi angett i denna integritetspolicy om du inte får annan information i samband med överlåtelsen

LAGLIG GRUND:

Intresseavvägning, eftersom vi bedömer att vårt intresse av att möjliggöra en förvärvs- eller omstruktureringsprocess överväger ditt intresse av skydd för dina personuppgifter. Det förutsätter dock att det övertagande bolaget bedriver liknande verksamhet som Edenred.

LAGRINGSTID:

Om Edenred upphör att existera, t.ex. genom en fusion, likvidation eller konkurs, eller om Edenreds kunddatabas överlåts till ett övertagande bolag kommer vi radera dina personuppgifter så länge vi inte behöver spara dem för att uppfylla lagkrav. Om Edenred förvärvas av ett övertagande bolag eller delas upp i samband med en omstrukturering kommer vi fortsätta spara och använda dina personuppgifter enligt villkoren i denna integritetspolicy, om du inte får annan information i samband med överlåtelsen.

DINA RÄTTIGHETER:

Du har rätt att invända mot sådan användning av dina personuppgifter som vi gör med stöd av en intresseavvägning. Se avsnitt 9 för att få information om dina rättigheter.[229]

Kommentar**:** Ovanstående skrivelse förefaller innefatta den information som är nödvändig enligt GDPR. Följaktligen kan skrivelsen potentiellt anses uppfylla undantaget som avser att de registrerade redan förfogar information vilket skulle innebär att informationen inte behöver lämnas ut i samband med ett företagsförvärv.

[229] Edenred AB.

Av de angivna exemplen på skrivelser i företags personuppgiftspolicys framgår att de flesta ej uppfyller kraven på den mängd information som krävs för att undantaget avseende att de registrerade redan förfogar över informationen ska vara uppfyllt. Det finns dock en skrivelse[230] som torde uppfylla villkoren för undantaget och således är en skrivelse av det slaget eftersträvansvärd för alla företag som skulle kunna tänkas genomföra ett företagsförvärv. Även fast all nödvändig information finns i en personuppgiftspolicy är det dock inte säkert att informationskravet anses uppfyllt med hänsyn till de höga krav som GDPR ställer på informationens tydlighet och begriplighet. I det fall att personuppgiftspolicyn är väldigt lång är det osannolikt att alla registrerade kommer att tillgodogöra sig informationen vilket skulle kunna få till följd att den anses brista i begriplighet och tydlighet. Därmed kan det sägas att GDPR i viss mån är motsägelsefull avseende informationskraven eftersom den föreskriver att en omfattande mängd information måste lämnas ut samtidigt som begripligheten av informationen tenderar att sjunka ju mer information som lämnas. En möjlig lösning på ovanstående problematik skulle kunna vara att ange sammanfattande information där de registrerade även får information om var de kan hitta mer djupgående information. Sammanfattningsvis kan det sägas att det finns möjlighet att uppfylla undantaget till informationskraven vad gäller tillförsäkrande av att de registrerade redan förfogar över informationen. För att kravet ska anses vara uppfyllt krävs en avvägning avseende förhållandet mellan den mängd information som lämnas och begripligheten av informationen.

[230] Edenred AB.

5. Sammanfattande slutsatser

5.1 Informationshanteringen vid en due diligence omfattas av GDPR

Vid informationshanteringen i samband med en due diligence förekommer det personuppgifter av det slag som omfattas av GDPR, bland annat i form av anställningsavtal och kundregister. Vidare kan det konstateras att informationshanteringen i samband med en due diligence är en personuppgiftsbehandling enligt GDPR, oavsett om ett manuellt eller virtuellt datarum används. Slutligen innehar samtliga aktörer i en due diligence antingen rollen som personuppgiftsansvarig eller personuppgiftsbiträde och omfattas därmed av GDPR:s ansvarsregler. Följaktligen måste reglerna i GDPR beaktas vid utförandet av en due diligence.

5.2 Rättslig grund för hantering av personuppgifter vid en due diligence

Att informationshanteringen vid en due diligence omfattas av reglerna i GDPR innebär att det krävs rättslig grund för att behandla personuppgifterna. De rättsliga grunderna som anges i artikel 6 är uttömmande och som framgår av ovanstående utredning är det inte möjligt att fastslå en rättslig grund som helt säkert är tillämplig vid alla due diligence-förfaranden. Utredningen visar på att det av olika anledningar kan vara problematiskt att förlita sig på samtycke som rättslig grund. Däremot kan intresseavvägningen beroende på omständigheterna i varje enskilt fall utgöra rättslig grund. För att öka sannolikheten för att en intresseavvägning ska resultera i rättslig grund kan åtgärder som exempelvis begränsning av antalet behandlade personuppgifter, pseudonymisering och anonymisering vidtas.

5.3 Vidtagande av säkerhetsåtgärder i samband med en due diligence

Som tidigare konstaterats är informationshanteringen i samband med en due diligence en personuppgiftsbehandling enligt GDPR. Förordningen medför därför krav på att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder. Minimering av personuppgiftsbehandling, pseudonymisering av personuppgifter, separat datarum för HR-avdelningen, utförliga sekretessavtal är alla exempel på åtgärder som kan vidtas. Det är inte möjligt att fastslå om det krävs att en konsekvensbedömning utförs eller ej vid en due diligence. Däremot har det konstaterats att en konsekvensbedömning alltid bör utföras i de situationer då den personuppgiftsansvarige är osäker på om det behövs eller ej. Vidare bör alltid en konsekvensbedömning utföras vid användning av ny teknik som till exempel AI.

5.4 Överföring av personuppgifter till annan personuppgiftsansvarig

En överföring av personuppgifter till en annan personuppgiftsansvarig som befinner sig inom EU är en vanlig personuppgiftsbehandling vilket medför att de sedvanliga reglerna för personuppgiftsbehandling är tillämpliga på en sådan överföring.

I det fall att en överföring av personuppgifter sker till en personuppgiftsansvarig som befinner sig utanför EU krävs, för att den ska vara lagenlig, att något av de villkor som finns i GDPR för tredjelandsöverföring är uppfyllt. Till att börja med följer det av ovanstående utredning att villkoren i artikel 49 förmodligen inte är tillämpliga. Vad gäller villkoret i artikel 45 om att det tredjelandet ska ha en adekvat skyddsnivå finns det inte så mycket för en personuppgiftsansvarig att göra förutom att vara uppmärksam på om överföringen sker till ett land med adekvat skyddsnivå eller ej. Villkoren i artikel 46 kan uppfyllas genom att ingå avtal med mottagaren som innehåller standardavtalsklausuler godkända av EU-kommissionen alternativt utforma egna avtalsklausuler som i sådant fall måste godkännas av Datainspektionen. Huruvida standardavtalsklausuler eller egenutformade avtalsklausuler är det bästa alternativet får avgöras utifrån de föreliggande omständigheterna i varje enskilt fall. Slutligen bör det observeras att antalet aktörer i en due diligence som befinner sig utanför EU

de senaste åren har ökat och dessutom finns det faktorer som talar för att dessa kommer att fortsätta öka varför reglerna är relevanta.

5.5 Uppfyllande av informationskravet i samband med en due diligence

Det har i utredningen konstaterats att informationskraven i artikel 13 och 14 GDPR måste uppfyllas vid informationshanteringen i samband med en due diligence. Dessutom har det konstaterats att det visserligen finns undantag från informationskraven men att det enda undantaget som förefaller vara tillämpligt i den situation som en due diligence innebär är att de registrerade redan besitter all nödvändig information. För tillförsäkra att de registrerade besitter informationen kan informationen återges i ett företags personuppgiftspolicy. I avsnitt 4.5.2 anges flera exempel på hur olika företag har utnyttjat sådana skrivelser i deras personuppgiftspolicys. För att uppfylla undantaget från informationskraven krävs en avvägning mellan mängden information som anges samt informationens begriplighet.

5.6 Generella slutsatser

Med hänsyn till ovanstående slutsatser råder det inget tvivel om att informationshanteringen i samband med en due diligence påverkas av reglerna i GDPR. På grund av att många av bestämmelserna i GDPR är beroende av omständigheterna i varje enskilt fall samt att det råder viss osäkerhet över hur de ska tolkas har det dock varit svårt att dra konkreta slutsatser avseende hur informationshanteringen påverkas av reglerna i GDPR. Däremot har det konstaterats att det finns flera olika åtgärder som en personuppgiftsansvarig bör vidta i samband med informationshanteringen vid en due diligence i syfte att se till att reglerna i GDPR efterlevs. I framtiden, i takt med att det kommer vägledning från EU-domstolen och en utveckling av doktrin, kommer det förmodligen att vara möjligt att dra skarpare slutsatser på området.

Käll- och litteraturförteckning

Offentligt tryck

Prop 1988/89:76 *om ny köplag*.

Prop. 2005/06:173 *Översyn av personuppgiftslagen*

Prop 2017/18: 105 *Ny dataskyddslag*

SOU 2017:39 *Dataskyddsutredningen*

EU-rättsligt material

Artikel 29-gruppen

Artikel 29-gruppen, WP 114, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October* 1995, Antagna den 25 november 2005. (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf) (Cit: Artikel 29-gruppen, WP 114.)

Artikel 29-gruppen, WP 169, *Opinion 1/2010 on the concepts of "controller" and "processor"*, Antagna den 16 feburari 2010. (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf) (Cit: Artikel 29-gruppen, WP 169.)

Artikel 29-gruppen, WP 217, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* Antagna den 9 april 2014. (https://www.dataprotection.ro/servlet/ViewDocument?id=1086) (Cit: Artikel 29-gruppen, WP 217.)

Artikel 29-gruppen, WP248, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679,* Antagna den 4 april 2017. (https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-konsekvensbedomning-avseende-dataskydd.pdf) (Cit: Artikel 29-gruppen, WP 248.)

Artikel 29-gruppen, WP 250, *Guidelines on Personal data breach notification under Regulation 2016/679,* Antagna den 3 oktober 2017. (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052)(Cit: Artikel 29-gruppen, WP 250.)

Artikel 29-gruppen, WP 259, *Guidelines on consent under Regulation 2016/679,* Antagna den 28 november 2017. (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051) (Cit: Artikel 29-gruppen, WP 259.)

Artikel 29-gruppen, WP 260, *Guidelines on transparency under Regulation 2016/679*, Antagna den 29 november 2017. (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227) (Cit: Artikel 29-gruppen, WP 260.)

EDPB

EDPB, *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679,* Antagna 25 maj 2018. (https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-undantag-enligt-artikel-49.pdf)(Cit: EDPB, Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679).

EDPB, *Infonote nodeal brexit*, Antagna den 12 februari 2019. (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en_0.pdf) (Cit: EDPB, *Infonote nodeal brexit.*)

Europeiska Kommissionen

Europeiska Kommissionen, *Adequacy decisions*. (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en) Hämtad: 2019-05-17. (Cit: Europeiska Kommissionen, *Adequacy decisions).*

Europeiska Kommissionen, *EU-US Data transfers.*(https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en) Hämtad: 2019-05-17. (Cit: Europeiska Kommissionen, *EU-US Data transfers*).

Europeiska Kommissionen, Kommissionens genomförandebeslut (EU) 2016/1250. (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016D1250&from=SV) Hämtad: 2019-05-17. (Cit: Kommissionens genomförandebeslut).

Europeiska Komissionen, *Opinons and recommendations.* **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm** Hämtad: 2019-05-17. (Cit: Europeiska Kommissionen, *Opinons and recommendations*)

Litteratur

Forssman, Magnus (2016). *Företagsöverlåtelser: En introduktion till den legala processen,* 2:a upplagan, Wolters Kluwers förlag, Stockholm. (Cit: Forssman (2016)).

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline och Beyer, Sandra (2018). *GDPR : juridik, organisation och säkerhet enligt dataskyddsförordningen*, 1:a upplagan, Norstedts Juridik, Stockholm. (Cit: Frydlinger m.fl. (2018)).

Holtz, Hajo Michael (2018). *Den nya allmänna dataskyddsförordningen — några anmärkningar,* SvjT 2018:240 s. 251.(Cit: Holtz(2018))

IT Governance privacy Team (2016), *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide,* IT governance publishing. (Cit: IT Governance Privacy Team (2016)).

Lindskog, Stefan(1990) i Unger, Sven och Thorsson, Leif (redaktionskommitté), *Festskrift till Gotthard Calissendorff*, Norstedt, Stockholm, 1990. (cit. Lindskog (1990))

Nääv, Maria. & Zamboni Mauro (2018). *Juridisk metodlära.* 2:a Upplagan, Studentlitteratur, Lund. (Cit: Nääv och Zamboni(2018)).

Ramberg, Christina(1992). *Kontraktsbrott vid köp av aktie - särskilt om fel*, Juristförlaget, Stockholm. (Cit: Ramberg (1992)).

Sevenius, Robert (2011). *Företagsförvärv: en introduktion*, Studentlitteratur, Lund. (Cit: Sevenius (2011)).

Sevenius, Robert (2013). *Due Diligence: Besiktning av företag*, Sanoma Utbildning, Stockholm. (Cit: Sevenius 2013)).

Tonell, Magnus (2012). *Sekretessavtal: och det rättsliga skyddet för företagshemligheter,* 1:a upplagan, Jure, Stockholm. (Cit: Tonell (2012)).

Voigt, Paul och von dem Bussche, Axel (2017), *The EU General Data Protection Regulation(GDPR) - A Practical Guide*, 1:a upplagan, Springer International Publishing, Cham, Schweiz. (Cit: Voigt & von dem Bussche (2017)).

Elektroniska källor

24solutions, *Pseudonymisering och anonymisering av persondata – vad är skillnaden?,* (https://www.24solutions.com/sv/blogg/pseudonymisering-anonymisering-persondata-skillnaden/) Hämtad: 2019-05-13. (Cit: 24solutions, *Pseudonymisering och anonymisering av persondata- vad är skillnaden?).*

Advokatsamfundet (2018), *Vägledning för tillämpning av EU:s dataskyddsförordning i advokatverksamhet*(https://www.advokatsamfundet.se/globalassets/advokatsamfundet_sv/advokatyrket/vagledning_for_tillampningen_av_eus_dataskyddsforordning_i_advokatverksamhet.pdf) Hämtad: 2019-05-13. (Cit: Advokatsamfundet (2018)).

Björkman, Fredrik (2019), Dagens Industri. *26,6 miljarder kronor - här är dundernotan för GDPR.*(https://digital.di.se/artikel/svenska-bolagens-nota-for-gdpr-266-miljarder-kronor) Publicerad: 2019-04-16. Hämtad: 2019-05-13. (Cit: Björkman (2019)).

Bolander, Hans (2019), Dagens Industri. *Vinge tar täten när företagsaffärer rivstartar* (https://www.di.se/nyheter/vinge-tar-taten-nar-foretagsaffarer-rivstartar/) Publicerad:2019-02-05. Hämtad: 2019-05-13. (Cit: Bolander(2019)).

Bolter, Linda (2019), Dagens Industri. *Larmet: Hundratusentals småföretag har noll koll på nya lagen- "beklämmande"* (https://www.di.se/nyheter/larmet-hundratusentals-smaforetag-har-noll-koll-pa-nya-lagen-beklammande/) Publicerad: 2019-05-15. Hämtad: 2019-05-17. (Cit: Bolter (2019)).

Datainspektionen, *Dataförordningens syfte och tillämpningsområde.*(https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-syfte-och-tillampningsomrade/). Hämtad 2019-05-13. (Cit: Datainspektionen, *Dataförordningens syfte och tillämpningsområde*).

Datainspektionen, *Datainspektionen leder arbete med nya EU-riktlinjer.* https://www.datainspektionen.se/nyheter/datainspektionen-leder-arbete-med-nya-eu-riktlinjer/) Hämtad: 2019-05-13. (Cit: Datainspektionen, *Datainspektionen leder arbete med nya EU-riktlinjer.)*

Datainspektionen, *Förteckning över när en konsekvensbedömning ska göras.* (*https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/*). Hämtad: 2019-05-13 (Cit: Datainspektionen, *Förteckning över när en konsekvensbedömning ska göras.*)

Datainspektionen, *Hur vidtar vi lämpliga skyddsåtgärder?* (*https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vidtar-vi-lampliga-skyddsatgarder/*). Hämtad: 2019-05-13 (Cit: Datainspektionen, *Hur vidtar vi lämpliga skyddsåtgärder?*).

Dataisnpektionen, *Så här är dataskyddet organiserat i EU.* (https://www.datainspektionen.se/om-oss/datainspektionens-internationella-arbete/sa-har-ar-dataskyddet-organiserat-i-eu/.) Hämtad: 2019-05-13. (Cit: Dataisnpektionen, *Så här är dataskyddet organiserat i EU*).

Person, Johan och Knutsson, (2017), Advokaten, nummer 1 2017, årgång 83, *Är din nästa kollega en robot?* (https://www.advokaten.se/globalassets/advokaten/1/advokaten2017_1.pdf), Hämtad:2019-05-13. (Cit: Person och Knutsson (2017)).

Höisteh, Patrik. (2019), Dagens Industri, *Svag krona ger rekordköp av svenska bolag* (https://www.di.se/nyheter/svag-krona-ger-rekordkop-efter-svenska-bolag/) Publicerad: 2019-03-25. Hämtad: 2019-05-13. (Cit: Höiseth(2019)).

Imprima, *Meet Imprima, The Leading Global SaaS Provider for Due Diligence, Asset Management and Docuement Sharing. (https://www.imprima.com/about/meet-imprima/)* Hämtad: 2019-05-13. (Cit: Imprima).

Johansson, Stefan (2018). *Konsekvensbedömning avseende dataskydd – riskanalys möter rättighetskrav,* Lov&Data 2018 nr. 4 s. 16–19. (https://lovdata.no/pro/#document/JUS/lod-2018-136-16?searchResultContext=1298&rowNumber=61&totalHits=185) Hämtad: 2019-05-13. (Cit: Johansson(2018)).

Karnov internet, artikel 6 GDPR, not 68. (https://pro.karnovgroup.se/document/2514469/5#CLX_3_2016_R_0679_N68) Hämtad: 2019-05-14. (Cit: Karnov internet, artikel 6 GDPR, not 68.)

Kira Systems, *Kira for due diligence,* (https://kirasystems.com/how-itworks/due-diligence/), Hämtad: 2019-05-14. (Cit: Kira Systems).

Larsson, Stefan och Ledendal, Jonas (2017), Konsumentverket, Rapport 2017:4, "Personuppgifter som betalningsmedel" (https://www.konsumentverket.se/globalassets/publikationer/produkter-och-tjanster/gemensamt/rapport-2017-4-personuppgifter-som-betalmedel-konsumentverket.pdf). Hämtad: 2019-05-13. (Cit: Larsson och Ledendal (2017)).

Merrill Corporation, *About Merrill. (https://www.merrillcorp.com/us/en/company.html)*. Hämtad: 2019-05-13. (Cit: Merill Corporation)).

Selbts, Vanessa. (2018), It-kanalen, *Utvecklingen inom AI går starkt framåt.*(https://it-kanalen.se/utvecklingen-inom-ai-gar-starkt-framat/) Publicerad: 2018-07-30 Hämtad: 2019-05-13. (Cit: Selbts (2018)).

Sevenius, Robert (2017), expertkommentar, *Tillämpningen av artificiell intelligens i due diligcence*, Blendow lexnova.(http://sevenius.se/publikationer/tillampningen-av-artificiell-intelligens-due-diligence-lexnova-mars-2017/) Hämtad: 2019-05-13. (Cit: Sevenius(2017)).

Personuppgiftspolicys

Dplay, Personuppgiftspolicy. (https://www.dplay.se/artiklar/personuppgiftspolicy) Hämtad: 2019-05-16 (Cit: Dplay AB).

Edenred, Personuppgiftspolicy.(https://www.edenred.se/juridiska-dokument/integritetspolicy-for-anstallda/) Hämtad: 2019-05-16. (Cit: Edenred AB).

Essity, Personuppgiftspolicy. (https://www.tork.se/juridisk-information/) Hämtad: 2019-05-16 (Cit: Essity AB).

Expedia, Personuppgiftspolicy. (https://www.expedia.se/p/support/privacy)Hämtad: 2019-05-16 (Cit: Expedia AB).

Ramirent, Personuppgiftspolicy. (https://www.ramirent.se/privacy) Hämtad: 2019-05-16 (Cit: Ramirent AB).

Sagax, Personuppgiftspolicy. (https://www.sagax.se/Global/Sverige/Om_AB_Sagax/Integritetsmeddelande%20externt%202018-05-24.pdf) Hämtad: 2019-05-16. (Cit: Sagax).

Visma, Personuppgiftpolicy. (https://www.visma.se/integritetspolicy/visma-som-personuppgiftsansvarig/hur-vi-delar-dina-personuppgifter/) Hämtad: 2019-05-16. (Cit: Visma).

Rättsfallsförteckning

EU-rätt

Mål C-524/06, *Heinz Huber mot Bundesrepublik Deutschland,* ECLI:EU:C:2008:724.

Mål C-131/12, *Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González,* ECLI:EU:C:2014:317.

Svensk rätt

NJA 1976 s. 341.