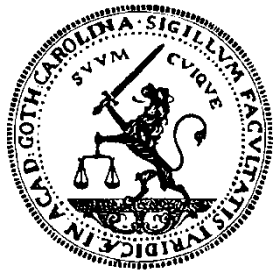

JURIDISKA FAKULTETEN
vid Lunds universitet

Hilda Cangemark

Antikorruptionsförebyggande tredjepartsbesiktning och GDPR

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Per Samuelsson

Termin för examen: Period 2 VT2019

Innehåll

Summary

Third party due diligence is an investigation of prospective or existing business partners in order to ensure a low risk of corruption. In certain countries such an investigation is required by law. Factors to consider in the risk assessment are for example whether a potential or existing business partner has been convicted of any corruption related crime or is associated with political circles. Swedish companies are questioning whether third party due diligence at all can be conducted due to GDPR, since the procedure involves the collection and processing of personal data. In Sweden, the provisions on negligent financing of bribery in The Swedish Penal Code and The Act on Transparency in the Financing of Political Parties involves a certain degree of duty to investigate or report. According to GDPR, criminal and sensitive personal data may be processed if required by a legal obligation, i.e. through EU law, national law or collective agreements. There is much to suggest that negligent financing of bribery can be considered a legal obligation that would allow third party due diligence. Regarding information on donors to political parties, the Data Protection Act appears to limit the scope of the provision of important public interest in art. 9.2 GDPR to a considerable extent only to authorities or otherwise if required by a company in the fulfillment of rights and obligations in, among other things, labor law.

The Swedish Data Protection Authority has been given considerable authority to draw up regulations, which according to both GDPR and Swedish preparatory work can be interpreted as an obligation for the authority to keep up to date on the development of the regulations and its consequences. It is therefore appropriate that the dilemma is resolved like the Irish solution, i.e. through a regulation from the Swedish Data Protection Authority, that would allow the processing of relevant personal data for the conduct of a third party due diligence. In a long-term perspective the government should, by law or extension of The Swedish Institute against Corruption mandate, establish regulations that in similarity with U.S., France and the U.K. require specific measures for the prevention of corruption in trade and industry.

Sammanfattning

Tredjepartsbesiktning innebär att blivande eller befintliga affärspartners undersöks i syfte att säkerställa att verksamhetsutövarens verksamhetsled utgör en låg risk för korruption, vilket i vissa länder krävs genom lag. Faktorer som i regel anses som varningsflaggor i riskbedömningen inför en affärstransaktion är till exempel om en affärspartner har dömts för något brott av korruptiv karaktär eller har någon anknytning till politiska kretsar. Svenska näringslivsaktörer ställer sig frågande till om tredjepartsbesiktning över huvud taget låter sig genomföras med anledning av GDPR, eftersom förfarandet innebär inhämtning och behandling av personuppgifter. I Sverige innebär bestämmelserna om vårdslös finansiering av mutbrott i 10 kap. 5 e § BrB och lag (2018:90) om insyn i finansiering av partier en viss grad av undersökningsplikt. Enligt GDPR får brottsuppgifter och känsliga personuppgifter behandlas om det krävs av en rättslig förpliktelse, dvs. genom unionsrätt, nationell rätt eller kollektivavtal. Det finns mycket som talar för att vårdslös finansiering av mutbrott kan anses utgöra en rättslig förpliktelse som skulle tillåta tredjepartsbesiktning. Vad gäller uppgifter om bidragsgivare till politiska partier tycks lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inskränka tillämpningsområdet för bestämmelsen om viktigt allmänt intresse som återfinns i art. 9.2 i GDPR avsevärt till att endast omfatta myndigheter eller annars om det krävs av en verksamhetsutövare i sin fullgörelse inom bland annat arbetsrätten.

Datainspektionen har fått stor befogenhet att upprätta föreskrifter, vilken genom både GDPR och svenska förarbeten kan tolkas som en skyldighet för myndigheten att hålla sig uppdaterad om regleringens utveckling och dess konsekvenser. Det ligger därför nära till hands att dilemmat löses genom en föreskrift från Datainspektionen som tillåter behandling av relevanta personuppgifter för genomförandet av tredjepartsbesiktning i likhet med den irländska lösningen. Ur ett långsiktigt perspektiv bör regeringen genom lag eller utvidgning av Institutet Mot Mutors uppdrag upprätta bestämmelser som i likhet med USA, Frankrike och Storbritannien på ett tydligt sätt kräver specifika åtgärder för att förebygga korruption i sin verksamhet.

Förord

GDPR är en stor suck, sa juristen och gick.

Den juristen får nog lov att vara jag.

Förkortningar

AFA Guidelines	Agence Française Anticorruption Guidelines
CPI	Corruption Perceptions Index
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
Dataskyddsförordningen	Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning
Dataskyddslagen	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
DIFS	Datainspektionens författningssamling
Ds	Departementsserie
EU	Europeiska Unionen
FCPA	Foreign Corrupt Practices Act
FN	Förenta Nationerna
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
GRECO	Council of Europe’s Group of States against Corruption
ICC	International Chamber of Commerce
Insynslagen	Lag (2018:90) om insyn i finansiering av partier
ISO	The International Organization for Standardization
Lagen om datainformation	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Näringslivskoden	Kod om gåvor, belöningar och andra förmåner i näringslivet
OECD	Organization for Economic Cooperation and Development
Prop	Proposition
Sapin II	LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique
SOU	Statens offentliga utredningar
U.K. Bribery Act	Bribery Act 2010 chapter 23
U.K. Data Protection Act	Data Protection Act 2018 chapter 12

1 Inledning

1.1 Bakgrund

Korruption har av *World Bank Group* och *World Economic Forum* uppskattats kosta samhället runt 3,6 biljoner amerikanska dollar globalt per år, varav en biljon utgör direkta mutor. Denna ungefärliga siffra har bekräftats av bland annat OECD år 2014 och av FN år 2018.[1] Europeiska kommissionen anförde i en rapport från 2014 att korruption inom EU kostar ungefär 120 miljarder euro per år, vilket motsvarar nästan hela EU:s årsbudget.[2] Eftersom korruption av sin natur sker i det dolda är det dock svårt att göra en exakt bedömning av omfattningen.[3] Rapporten visar även att omkring fyra av tio företag inom EU anser att korruption är ett problem för affärsverksamheten. Inom bygg-, telekom- och IT-sektorn ansåg hälften respektive en tredjedel av de tillfrågade företagen korruption utgöra ett allvarligt problem för affärsverksamheten.[4]

Korruption utgör ett allvarligt hot mot den allmänna tilliten i dagens ekonomi och samhälle, bland annat genom att relationer mellan aktörer på marknaden skadas vilket undergräver marknadsekonomin. På marknaden eftersträvas erkända och goda villkor tillsammans med säkra och pålitliga valutor, stabila former för valutaväxling samt legala möjligheter för tvistlösning och möjlighet att hävda sin rätt.[5] För att bekämpa korruption är det inte tillräckligt med enbart regelverk, utan även hög integritet hos inblandade marknadsaktörer krävs. Det leder till frågan om nödvändigheten av god moral i näringslivet.[6]

---

[1] Network of Global Agenda Councils Reports 2011 – 2012 (Anti-corruption), se bland annat OECD https://www.oecd.org/cleangovbiz/49693613.pdf; World Economic Forum http://reports.weforum.org/global-agenda-council-2012/councils/anti-corruption/; FN https://news.un.org/en/story/2018/12/1027971; World Economic Forum https://www.weforum.org/agenda/2018/12/the-global-economy-loses-3-6-trillion-to-corruption-each-year-says-u-n/; samtliga hämtade 2019-08-06.
[2] EU:s rapport om insatserna mot korruption, s. 3.
[3] Borglund m.fl., s. 208.
[4] EU:s rapport om insatserna mot korruption, s. 7.
[5] Borglund m.fl., s. 207 ff.
[6] Ibid, s. 208.

För att förebygga korruption i sin verksamhet används complianceprogram. Det innebär att organisationen frivilligt sätter ramar för vilket beteende som tolereras inom verksamheten och regler för hur oacceptabelt beteende ska förebyggas, förhindras och rapporteras. Reglerna kan innebära en skyldighet att utföra riskbedömningar, uppförandekoder, utbildningsprogram, efterlevnadskontroller, hållbarhetsrapporter och genomförande av disciplinära åtgärder.[7]

Ett annat tillvägagångssätt för att förhindra finansiella oegentligheter är att införa lagkrav på åtgärder som varje verksamhet måste vidta i förebyggande syfte. Denna typ av reglering är vanlig inom områden som dataskydd, läkemedelsproduktion, finansiella tjänster och hälsovård.[8] Lagregleringarna inom nämnda områden omfattar verksamhetens ansvar vid anställdas korrupta handlingar, samt personligt ansvar för verksamhetsledningen vid misslyckad implementering av relevant complianceprogram.[9] Enligt professor Sharon Oded är reglering som siktar på skyldigheten att vidta åtgärder i ett förebyggande syfte inte särskilt vanligt i länder inom EU, som istället tycks välja regelsystem som siktar på utdömande av ansvar efter en vidtagen korrupt handling. Undantaget från detta är till exempel Storbritannien och Frankrike, som i likhet med USA har infört riktlinjer för eller krav på existensen av och innehållet i complianceprogram.[10]

Gemensamt för dessa länder är att deras regelverk påkallar tredjepartsbesiktning[11], vilket normalt utgör en viktig komponent för *compliance*. Tredjepartsbesiktningen innebär att blivande eller befintliga affärspartners undersöks i syfte att säkerställa att dennes verksamhets utgör en låg risk för korruption. Förfarandet kan antingen genomföras av verksamheten internt eller genom en utomstående part vars expertis ligger inom området. Oded är av uppfattningen att anlitandet av en utomstående

[7] Oded, s. 101 not 1; Borglund m.fl., s. 247.
[8] Oded, s. 101.
[9] Ibid, s. 102.
[10] Ibid, s. 157.
[11] *Eng. third party due diligence.*

expert är det mest effektiva tillvägagångssättet för ett proaktivt compliancearbete.[12]

För att bedöma risker med affärsavtal måste vissa faktorer identifieras. Faktorer som bör anses utgöra varningsflaggor är till exempel om en potentiell eller befintlig affärspartner har varit under utredning eller dömts för brott av korruptiv karaktär eller har någon anknytning till politiska kretsar. Verksamheter kan hamna i en situation där ett gediget compliancearbete enligt lag måste utföras inför varje affärstransaktion, och där restriktioner för personuppgiftsbehandling enligt Europaparlamentets och rådets förordning 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (GDPR) samtidigt gör sig gällande. Aktörer inom näringslivet ställer sig då frågande till om tredjepartsbesiktning överhuvudtaget låter sig genomföras, eftersom det innebär inhämtning och behandling av personuppgifter potentiellt i strid med GDPR. Med anledning av rädsla för att åläggas sanktioner i form av företagsböter på miljonbelopp samt personlig böter och fängelse för verksamhetsledningen, å ena sidan på grund av krav på tredjepartsbesiktning och å andra sidan restriktioner enligt GDPR, vittnar svenska näringslivsaktörer om ett dilemma som kan resultera i ett dödläge på den globala marknaden.

1.2 Syfte och frågeställningar

Uppsatsen syftar till att utreda om det föreligger en regelkonflikt mellan tredjepartsbesiktning och GDPR, inom ramen för organisationers förebyggande antikorruptionsarbete. Om en sådan konflikt kan konstateras utreds möjliga problemlösningar som kan göras gällande i Sverige, med inspiration av regelverk från fyra olika länder; Storbritannien, Irland, Frankrike och USA. Uppsatsen syftar även till att erbjuda en översikt hur dessa regelverk är uppbyggda.

[12] Oded, s. 246.

- Ställer GDPR upp hinder för tredjepartsbesiktning? Om så är fallet, finns några undantag?
- Hur har andra länder som lyder under antikorruptionsregelverk och GDPR löst en eventuell konflikt?
- Finns det underlag i svensk rätt för genomförande av tredjepartsbesiktning genom undantagen i GDPR? Om nej, hur skulle en eventuell konflikt kunna lösas och se ut i Sverige?

1.3 Metod och material

För att uppnå syftet med uppsatsen granskas regelverkens relevanta innehåll för att identifiera en eventuell konflikt. För att exemplifiera ett kraftigt regelverk används USA:s antikorruptionsregelverk FCPA som verktyg. Om en konflikt kan konstateras ämnar uppsatsen till att presentera en potentiell lösning. För ledning i en sådan problemlösning undersöks relevanta regelverk i länder som dels lyder under GDPR, dels har inrättat ett krävande antikorruptionsregelverk. De europeiska länderna som har valts i arbetet är Irland, Storbritannien och framförallt Frankrike. Nämnda länder har hanterat frågan på olika utförliga nivåer, vilket lämpar sig för uppsatsens jämförelser. Metoden har alltså genomförts med inslag av ett komparativt perspektiv med syfte att identifiera och belysa de största utmaningarna mellan regelverken, men även för att identifiera de bästa lösningarna som kan fungera som mall för en svensk modell.[13] Med det sagt har inte en komparativ metod använts i egentlig mening, eftersom arbetet inte går ut på att analysera likheter och skillnader mellan diverse regelverk eller att skapa en gemensam begreppsram för tredjepartsbesiktning, utan snarare presenterar respektive länders lösningar på aktuella problem.[14]

Behandlingen av materialet för utredningen utförs med en rättsanalytisk metod, primärt av den anledningen att relevant litteratur återfinns inom andra vetenskaper än den rättsvetenskapliga, framförallt den statsvetenskapliga och ekonomiska vetenskapen. Den rättsanalytiska metoden har till syfte att utreda

[13] Kleineman, s. 41 ff.
[14] Valguarnera, s. 143 och 167 med där hänvisningar.

vad som är gällande rätt, men begränsar sig inte till auktoritativa källor såsom lag, förarbeten och rättspraxis. Istället syftar den rättsanalytiska metoden till att analysera rätten utifrån en mer omfattande mängd material och är följaktligen inte lika begränsad som den rättsdogmatiska metoden.[15] Den rättsanalytiska metoden tillåter att analysen bygger på material från andra vetenskaper, inofficiell rätt och annan så kallad *soft law*, till exempel normer i näringslivet, uppförandekoder[16], nämndbeslut samt rekommendationer från internationella organ.[17] Eftersom korruption och *compliance* till stor del har behandlats i den ekonomiska och statsvetenskapliga forskningen och litteraturen, och som regel får relevans för jurister först vid praktiskt yrkesutövande genom *soft law* eller utrikes regelverk, är den rättsanalytiska metoden lämplig. Litteraturen som används i arbetet inom ramen för korruption och *compliance* är till största del dessutom skriven utifrån ett interdisciplinärt perspektiv.

GDPR, som också utgör en stor del av verksamhetsutövares compliancearbete, återfinns i den juridiska litteraturen. I den litteratur som finns att tillgå har dock trycksvärtan knappt hunnit torka, och har till största del enbart en beskrivande karaktär av förordningens innehåll. Därför har Sören Ömans kommentarer till GDPR varit en värdefull tillgång under arbetet. Regelverket är så pass nytt att några direkta effekter, förutom utmaningen att leva upp till regelverket, ännu inte har kunnat analyseras tillräckligt. För att nå den juridiska kärnan så nära som möjligt har informationen därför hämtats direkt från förordningen, svenska förarbeten och Artikel 29-gruppens yttrande inför förordningens införande.[18] Med anledning av nyss nämnda förekommer således inslag av EU-rättslig metod i arbetet, i syfte att undersöka och tydliggöra det bakomliggande syftet med relevanta bestämmelser i förordningen.[19]

[15] Sandgren (2018), s. 45 f.
[16] *Eng. code of conduct.*
[17] Sandgren (2016), s. 724 f.
[18] Artikel 29-gruppen syftade till att agera rådgivande, oberoende och övervakande över medlemsstaternas tillämpning av förordningen. Gruppen är sedan maj 2018 ersatt av Europeiska dataskyddsstyrelsen, för mer information se https://edpb.europa.eu/edpb_sv.
[19] Reichel, s. 109 ff.

De översättningar som har krävts från engelska och franska till svenska är inte officiella översättningar utan mina egna.

1.4 Avgränsningar

Uppsatsen är avgränsad till att behandla de regler som gör gällande tredjepartsbesiktning ur ett antikorruptionsperspektiv. I svensk bemärkelse rör det sig främst om vårdslös finansiering av mutbrott, även om andra handlingar kan utgöra korrupt beteende. Uppsatsen är därmed avgränsad till att behandla de bakomliggande syftena för vårdslös finansiering av mutbrott och till viss del även insyn i partiers finansiering. Uppsatsen berör således inte visselblåsarsystem, penningtvätt, skatterättsliga aspekter eller straffrättsliga aspekter, utöver beskrivandet av vilka påföljder som kan aktualiseras vid negligerad tredjepartsbesiktning. Sveriges internationella åtaganden mot korruption benämns endast i ett för läsaren upplysande syfte avseende existensen av dessa. Uppsatsen utreder inte mellan- eller överstatliga förpliktelser som uppstår genom internationella konventioner mot korruption och inte heller konsekvenser som kan aktualiseras om konventionerna inte efterlevs.

Uppsatsen behandlar inte behöriga myndigheter vars personuppgiftsbehandling omfattas av Europaparlamentets och Rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF. Vidare berör inte uppsatsen rättigheter som tillfaller individer i GDPR som till exempel rätt till radering och invändning mot personuppgiftsbehandling.

Irländsk, brittisk och fransk lagstiftning beskrivs i den mån som behövs för att utreda och visa hur tredjepartsbesiktning och GDPR regleras i förhållande till varandra. Det amerikanska regelverket beskrivs i den mån det påvisar kraven för det förebyggande antikorruptionsarbetet, och på så sätt krockar

med krav uppställda i GDPR. Någon vidare utredning av den amerikanska lagstiftningens innebörd förekommer inte.

1.5 Disposition

Inledningsvis beskrivs korruption och dess påverkan på samhället för att ge läsaren en grundläggande introduktion till det breda ämnet. Första kapitlet syftar till att beskriva varför det är viktigt att bekämpa korruption och på vilka sätt Sverige genom nationell och internationell reglering arbetar för detta. Andra kapitlet beskriver GDPR från unionsrättens perspektiv och hur regelverket tolkas i Sverige. Följt av den unionsrättsliga och svenska beskrivningen av GDPR utreds tredjepartsbesiktning utifrån svensk, irländsk, brittiskt, fransk och amerikansk rätt i kapitel fyra. Avslutningsvis i kapitel 5 ställs tredjepartsbesiktning i förhållande till GDPR för att besvara frågeställningarna, där det främst analyseras huruvida svensk reglering inom antikorruptionsområdet utgör tillräckligt stöd för att klassificeras som ett undantag i GDPR:s mening.

Flertalet engelska begrepp kan påstås vara allmänt vedertagna i den internationella antikorruptionsdoktrinen. Dessa har översatts till svenska i den mån begreppet ifråga inte förlorar sin betydelse. Begreppet personuppgiftsansvarig är hämtat från GDPR och avser i arbetet den verksamhetsutövare som behandlar personuppgifter.

2 Korruption

2.1 Definition

Korruption är inte ett rättsligt begrepp, utan kan istället konstateras vara ett samlingsbegrepp för otillbörliga förfaranden i relationer mellan aktörer.[20] Svenska Akademien definierar begreppet korruption bland annat som fördärv, systematiskt missbruk av ansvarsfull ställning i eget intresse och mottaglighet för mutor.[21] Nationalencyklopedin definierar korruption som missbruk av förtroendeställning för egen vinning, och något som ”…*är ett stort problem i länder där det saknas tradition av lojalitet mot uppdragsgivare”*.[22] Korrupt beteende kan ta sin form på många olika sätt, till exempel genom mutor, nepotism, marknadsmissbruk och kreativ bokföring.[23]

2.2 Sverige

Enligt *Transparency Internationals* årliga CPI kan den allmänna uppfattningen att korruption inte är vanligt förekommande i den svenska offentliga sektorn utläsas. Någon undersökning för den privata sektorn genomförs inte, men viss ledning kan tas av undersökningen för att få ett generellt grepp om samhällets uppfattning om förekommande korruption. Undersökningen omfattar 180 geografiska områden, vilka rankas av experter på en skala 0 till 100, där 0 innebär *highly corrupt* och 100 *very clean*. I 2018 års CPI rankas Sverige på skalan 85 av 100, vilket innebär en tredjeplacering som renast land på listan över de 180 undersökta länderna. Den svenska placeringen har under de senaste fyra åren varierat mellan 89 och 84 av 100.[24] Detta trots senaste årens rapportering om omfattande korruption i svenska

[20] Sundstrand, s. 108.
[21] Se *Korruption*, Svenska Akademiens Ordbok. Finns att läsa här https://svenska.se/tre/?sok=korruption&pz=1, besökt 2019-08-06.
[22] Se *Korruption*, Nationalencyklopedin. Finns att läsa här https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/korruption, besökt 2019-08-06.
[23] Se t.ex. https://www.institutetmotmutor.se/kunskapsbank/ordlista/korruption/; https://www.transparency.se/korruption, samtliga besökta 2019-08-06; Borglund m.fl., s. 211.
[24] Corruption Perception Index 2018, Transparency International. Finns att granska här https://www.transparency.org/cpi2018, besökt 2019-08-06.

organisationer som till exempel Telia, Statens Fastighetsverk, Trafikverket, Swedbank, Systembolaget och SAAB.[25]

År 2012 infördes dagens regler för mutbrott och vårdslös finansiering av mutbrott i Brottsbalkens 10 kap. Genom förarbeten till bestämmelserna utses Institutet Mot Mutor till förvaltare av Näringslivskoden, för att agera vägledande i näringslivet vad gäller representation och gåvor för undvikandet av mutbrott. Syftet var att ge näringslivet en självreglerande funktion.[26] Europeiska kommissionen belyser dock i sin rapport från 2014 att Sverige saknar en nationell strategi för att bekämpa korruption, men att vissa riskbedömningar och rapporter har genomförts. Dessa har främst berört den offentliga sektorn. Sveriges styrka konstateras i rapporten ligga i de grundläggande principerna avseende statsskicket som till exempel öppenhet och insyn, i kombination med en stor respekt för rättsstaten.[27] GRECO påpekade i sin rapport från 2019 att det förvisso förekom en låg andel mutbrott, men desto mer av vänskapskorruption. GRECO ansåg det nödvändigt att Sverige antar och implementerar strategier för att motverka vänskapskorruption för att förhindra jävssituationer och för att öka graden av integritet, särskilt för högt uppsatta statstjänstemän och anställda inom polismyndigheten. GRECO rapporterade också att transparensen måste öka vad gäller högt uppsatta statstjänstemäns kontakter med tredjeparter, inklusive lobbyister.[28] Sammanlagt påkallar GRECO 15 åtgärder i sin rapport, vilka kommer att följas upp år 2021.[29]

---

[25] Se till exempel *Telia*: Stockholms tingsrätts dom 2019-02-15 i mål nr B 122201-17; https://www.svd.se/telias-mutharva-i-uzbekistan-detta-har-hant-xycx; *Statens Fastighetsverk*: https://www.svt.se/nyheter/inrikes/korruptionsskandalen-pa-statens-fastighetsverk-detta-har-hant, hämtad 2019-08-06; *Trafikverket*: Umeå tingsrätts dom 2019-02-21 i mål nr B 2793-17; https://www.svd.se/vagmalare-vittnar-om-mutor-pa-trafikverket; https://omni.se/utredning-om-mutbrott-pa-trafikverket-i-umea/a/kaR7ok, hämtade 2019-08-06; *Swedbank*: https://www.svt.se/special/swedbank/; https://www.dn.se/ekonomi/korruptionsexpert-swedbank-riskerar-att-utestangas-fran-internationell-handel/, hämtade 2019-08-06; *Systembolaget*: https://sverigesradio.se/sida/avsnitt/1174260?programid=2519; https://press.systembolaget.se/systembolaget-fortsatter-bekampa-korruption-trots-skadestand-i-ny-dom/, hämtade 2019-08-06; *SAAB*: Hovrätten för Västra Sveriges dom 2018-02-06 i mål nr B 2742-17; https://www.svd.se/saab-anmals-for-mutbrott--hogsta-cheferna-kan-forhoras, hämtad 2019-08-06.

[26] SOU 2010:38, s. 205.

[27] EU:s rapport om insatserna mot korruption, Annex 27, Bilaga Sverige, s. 2.

[28] GRECO, Evaluation report Sweden, s. 4.

[29] Ibid, s. 44.

2.3 Internationella initiativ

2.3.1 Mellan- och överstatliga initiativ

Sverige ingår i flera mellan- och överstatliga initiativ för att bekämpa korruption, till exempel FN-konventionen mot korruption och OECD.[30] OECD har utarbetat ett flertal regelverk, bland annat *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*, *Guidelines for Multinational Enterprises* och *Due Diligence Guidance for Responsible Business Conduct,* varav de två senare riktar sig till globala verksamhetsutövare istället för medlemsstaten. [31] Sverige är också anslutna till GRECO, vilket upprättades av Europarådet för övervakning av medlemsstaternas efterlevnad av bland annat Civil Law Convention on Corruption och Criminal Law Convention on Corruption.[32]

2.3.2 Privata initiativ

ISO är en organisation som fastställer åtgärder för anslutande organisationer att vidta för att förhindra korruption i sin verksamhet. Ett av dessa regelverk är ISO 37001 *Anti-bribery management systems - Requirements with guidance for use* vilket ställer krav på verksamhetens ledning att upprätta ramverk som inte bara förbjuder mutor, utan även fastställer granskning och förebyggande av mutor.[33] *Due diligence* beskrivs i regelverket som en process för att ytterligare bedöma typen och omfattningen av risken för mutor samt

[30] General Assembly resolution 58/4 of 31 October 2003 United Nations Convention against Corruption. Finns att läsa här https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf besökt 2019-08-06; Convention on the Organisation for Economic Co-operation and Development, Paris 14th December 1960. Finns att läsa här https://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm, besökt 2019-08-06.
[31] OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 17 December 1997. Finns att läsa här http://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf, hämtad 2019-08-06; OECD Guidelines for Multinational Enterprises, 2011 edition. Finns att läsa här http://www.oecd.org/daf/inv/mne/MNEguidelinesSVENSKA.pdf, hämtad 2019-08-06; OECD Due Diligence Guidance for Responsible Business Conduct, 31 May 2018. Finns att läsa här https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf, hämtad 2019-08-06. Fler riktlinjer för specifika verksamhetssektorer finns att läsa här http://mneguidelines.oecd.org/mneguidelines/, hämtad 2019-08-06.
[32] https://www.coe.int/en/web/greco/about-greco/priority-for-the-coe, besökt 2019-08-06.
[33] 5.2 Policy mot mutor ISO 37001:2017.

att hjälpa organisationer att ta beslut gällande specifika transaktioner, projekt, aktiviteter, affärspartners och personal.[34]

ICC har upprättat *Rules on Combating Corruption* som är en självreglering för verksamheter, för upprätthållandet av en god och etisk verksamhetsutövning. Självregleringen innebär bland annat utförande av *due diligence* avseende samtliga berörda parter i verksamheten i förhållande till de korruptionsrisker som finns eller de omständigheter som uppställs i regelverket. I detta ingår också att vid affärsrelationer uppmuntra att samtliga parter agerar i enlighet med regelverket.[35]

[34] P. 3.30 due diligence, ISO 37001:2016.
[35] Art. 10.g ICC Rules on Combating Corruption. Finns att läsa här https://cdn.iccwbo.org/content/uploads/sites/3/2011/10/ICC-Rules-on-Combating-Corruption-2011.pdf, hämtad 2019-08-06.

3 GDPR

3.1 Bakgrund och syfte

Skyddet för individers personuppgifter är en grundläggande rättighet enligt art. 8.1 i Europeiska unionens stadga om de grundläggande friheterna och art. 16.1 i Europeiska unionens funktionssätt.[36] Den fria inre marknaden i kombination med globalisering och en snabbt framåtskridande teknisk utveckling innebär ett behov av reglering avseende insamling och överföring av personuppgifter, eftersom utbytet av personuppgifter mellan såväl privata som offentliga aktörer ökar i takt med utvecklingen.[37] För att behålla den tillit för den inre marknaden som krävs för en fortsatt digital och ekonomisk utveckling bör fysiska personer ha kontroll över sina egna personuppgifter.[38]

GDPR syftar till att bidra till att skapa frihet, säkerhet och rättvisa inom unionen, med ekonomisk konvergens och utveckling i den fria marknaden men även avseende fysiska personers välbefinnande.[39] Vad som eftersträvas är därmed en enhetlig och hög skyddsnivå för individers personuppgifter i unionens medlemsstater.[40] Regleringen innebär att verksamhetsutövare måste inhämta individers samtycke eller på annat sätt ha laglig grund för att behandla personuppgifter.[41]

3.2 Rättslig innebörd

Varje inhämtning och behandling av personuppgifter måste vara laglig och rättvis. Hur personuppgifterna behandlas ska klart och tydligt framgå för varje berörd individ, inklusive hur uppgifterna kan behandlas i framtiden. Informationen ska vara lättillgänglig, lättbegriplig och sörja för en rättvis och öppen behandling av uppgifterna. Varje individ som lämnar sitt samtycke till uppgiftsbehandlingen bör göras uppmärksammad på de risker, regler,

[36] Skäl 1 GDPR.
[37] Skäl 5 och 6 GDPR.
[38] Skäl 7 GDPR.
[39] Art. 1 och skäl 2 GDPR.
[40] Skäl 10 GDPR.
[41] Art. 7 och skäl 32 GDPR.

skyddsåtgärder och rättigheter som behandlingen innebär. Uppgiftsbehandlingens ändamål bör även tydligt framgå när personuppgifterna samlas in.[42] Individen har rätt att ta del av de insamlade personuppgifterna som rör denne själv, samt begära rättelse och radering av uppgifterna och begränsning av behandling av uppgifterna.[43] Rättigheter och skyldigheter enligt GDPR kan dock begränsas genom unionsrätten eller nationell rätt om det sker av till exempel säkerhetsskäl, straffrättsliga skäl, ekonomiska eller finansiella intressen och för utförande av etiska åligganden för yrkesroller.[44] Insamling och behandling av personuppgifter bör endast utföras då ändamålet inte rimligen kan uppnås genom annat tillvägagångssätt, vilket ställer krav på adekvans, relevans och nödvändighet.[45]

3.3 Tillämpningsområde

GDPR omfattar behandling av personuppgifter som sker både automatiserat och manuellt.[46] I Sverige definieras automatiserad behandling kortfattat som en behandling och överföring av personuppgifter i datorformat.[47] Med manuell behandling avses annan än automatiserad behandling som innebär att personuppgifter ingår i ett regelrätt register, till exempel genom enkäter eller muntlig insamling.[48] Skyddet som tillhandahålls genom GDPR avser endast fysiska personer, oberoende av hemvist eller medborgarskap.[49] Skyldighet att följa regleringen åligger alla verksamheter etablerade inom EU som inom ramen för yrkes- eller näringsverksamhet införskaffar och behandlar personuppgifter. För verksamheter som inte är etablerade inom EU gäller GDPR enbart viss personuppgiftsbehandling. Det måste vara fråga om personuppgifter som tillhör en person som fysiskt befinner sig inom EU och att personuppgiftsbehandlingen har en anknytning till utbjudande av varor och tjänster till personer inom EU eller till övervakning av registrerade personers beteende så länge detta beteende sker inom EU. GDPR omfattar

[42] Art. 12–14 och skäl 39 GDPR.
[43] Art. 15–18 GDPR.
[44] Art. 23.1 GDPR.
[45] Art. 5 och skäl 39 GDPR.
[46] Art. 2 GDPR.
[47] SOU 1997:39, s. 344.
[48] SOU 2009:44, s. 94 ff.
[49] Skäl 14 GDPR.

också verksamheter som är etablerade i ett territorium där en medlemsstats nationella rätt gäller enligt folkrätten, till exempel på diplomatiska beskickningar eller konsulat.[50]

Den svenska kompletteringen av GDPR sträcker sig utöver unionsrätten på så vis att fler verksamheter omfattas av skyldigheten att följa regelverket rent extraterritoriellt.[51] I förarbetet föreslås GDPR vara av subsidiär karaktär i förhållande till sektorsspecifika författningar, utan att för den sakens skull utvidga utrymmet för nationella undantag enligt GDPR. Principen om unionsrättens företräde innebär att en sektorsspecifik författning endast får tillämpas då det är förenligt med, i detta fall, de i GDPR föreskrivna undantagen.[52]

3.4 Tillsyn

Varje medlemsstat ska utse eller upprätta en tillsynsmyndighet med behörighet och befogenhet att upprätthålla skyddet för personuppgifter, vilket i Sverige är Datainspektionen.[53] Inom medlemsstatens territorium bör tillsynsmyndigheten utöva tillsyn inom ramen för personuppgiftsbehandling vid myndigheter och privata aktörer verksamma inom territoriet, som antingen agerar i ett allmänt intresse eller utför en personuppgiftsbehandling som berör medlemsstatens medborgare, eller när en aktör etablerad i tredje land behandlar medlemsstatens invånares personuppgifter.[54] Tillsynsmyndigheten bör enligt skälen till GDPR även ha behörighet att anta bindande beslut inom ramen för de befogenheter som tilldelas genom GDPR.[55] Befogenheter som tilldelas genom GDPR är bland annat undersökningsbefogenhet, korrigerande befogenhet, befogenhet att ålägga sanktioner och utfärda tillstånd och verka rådgivande, samt att införa tillfälliga eller definitiva begränsningar av eller förbud mot

[50] Art. 2.2 a-c GDPR; Öman, s. 48 ff.
[51] SOU 2017:39, s. 20 och 92.
[52] Ibid, s. 84 f.
[53] Art. 51.1, 55 och skäl 117 GDPR; 2 a § Förordning (2018:1286) om ändring i förordningen (2007:975) med instruktion för Datainspektionen.
[54] Skäl 122 GDPR.
[55] Skäl 125 GDPR.

personuppgiftsbehandling.[56] Det åligger också tillsynsmyndigheten att följa utvecklingen inom relevanta områden som berör personuppgifter, vilket till exempel kan omfatta informations- och kommunikationsteknik och branschpraxis.[57]

Vid överträdelse av skyldigheterna enligt GDPR kan den personuppgiftsansvarige åläggas administrativa sanktionsavgifter upp till 20 miljoner euro eller fyra procent av den globala omsättningen föregående budgetår. Vilken sanktionsavgift som ska användas beror på vilken som utgör det högsta värdet.[58] Undantaget från detta är myndigheter, där sanktionsavgiften istället ligger på maximalt 10 miljoner svenska kronor (kr) enligt lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Medlemsstaten får utöver dessa administrativa sanktionsavgifter förelägga ytterligare sanktioner.[59] Utöver sanktionsavgifter kan personuppgiftsansvariga bli skadeståndsskyldig i förhållande till den person som lidit materiell eller immateriell skada på grund av överträdelse av GDPR.[60] GDPR bidrar dock inte med någon vägledning till hur skadeståndet ska beräknas. I Sverige har skadeståndet betraktats som en kränkningsersättning, vilket utgår från den skadelidandes känslor och behov av upprättelse. Mindre allvarliga kränkningar har värderats till ett skadeståndsvärde om 3000 kr, vilket ska ses som ett schablonbelopp.[61] Om en administrativ sanktionsavgift anses som alldeles för betungande för den personuppgiftsansvariga som vidtagit överträdelsen av GDPR, får tillsynsmyndigheten istället utfärda reprimander.[62]

GDPR föreskriver inte uttryckligen vilka typer av verksamheter som omfattas av förordningen, utan framgår istället delvis genom praxis. I C-101/01 *Lindqvist* konstaterades att undantagens tillämpningsområde begränsas till de verksamheter som uttryckligen nämndes i det då gällande

[56] Art. 57, 58 och skäl 129 GDPR.
[57] Art. 57.i GDPR.
[58] Art. 83.1, 83.4 och 83.5 GDPR.
[59] Art. 84.1 GDPR.
[60] Art. 82 GDPR; Frydlinger m.fl., s. 331 f.
[61] Frydlinger m.fl., s. 333.
[62] Skäl 148 GDPR.

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (Dataskyddsdirektivet), eller sådan verksamhet som kan placeras i samma kategori.[63] Myndighetsverksamhet som syftar till att förebygga, förhindra, utreda, avslöja och lagföra brott omfattas inte av GDPR.[64]

3.5 Laglig behandling av personuppgifter

Art. 6 föreskriver de villkor som gäller för att lagligen behandla personuppgifter. Till en av dessa villkor ska de kumulativa grundläggande principerna i art. 5 uppfyllas, vilka är laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering och slutligen integritet och sekretess. Vad gäller behandling av personuppgifter som omfattas av känsliga uppgifter i art. 9.2 och brottsuppgifter i art. 10 krävs det ytterligare rättslig grund för laglig behandling.[65] Individers samtycke utgör redan genom GDPR en rättslig grund för behandling av personuppgifter, förutom i de fall som avser behandling av personuppgifter för att fullgöra en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning för en personuppgiftsansvarig.[66] Under nämnda omständigheter krävs att medlemsstaterna gör personuppgiftsbehandlingen tillåtlig genom lagreglering.[67] I Sverige får sådana personuppgifter även behandlas om det uttryckligen tillåts genom förordning eller av Datainspektionen utfärdade föreskrifter eller förvaltningsbeslut.[68]

Myndigheter behöriga att behandla personuppgifter vars ändamål omfattas av GDPR, får i den nationella rätten förses med specifika och anpassade tillämpningsbestämmelser av personuppgiftsbehandlingen. Privata aktörer

[63] Domstolens dom den 6 november 2003 i mål C-101/01, EU:C:2003:596; SOU 2017:39, s. 88.
[64] Art. 2.2.d, skäl 18, 19 och 22 GDPR.
[65] Art. 5.1 a-f GDPR; Öman, s. 147 ff.
[66] Art. 6.1 och skäl 10 GDPR.
[67] Art. 6.2 och skäl 40 GDPR.
[68] Prop. 2017/18:105, s. 48 ff.

som behandlar personuppgifter får under vissa förutsättningar undantas från skyldigheterna enligt GDPR i nationell rätt. Det innebär att undantaget måste utgöra en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle för att skydda särskilda allmänna intressen som till exempel förebyggande, förhindrande, utredande, avslöjande och lagföring av brott eller hot mot den allmänna säkerheten.[69] I skälen till GDPR exemplifieras förebyggande och bekämpning av penningtvätt som ett sådant relevant intresse.[70]

3.5.1 Ändamålsenlighet

Behandling av personuppgifter får användas för andra ändamål än ursprungligen åsyftat om ändamålen kan anses förenliga med det ursprungliga ändamålet. För detta krävs inte någon ytterligare rättslig grund än den ursprungliga. Om en personuppgiftsbehandling däremot är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning kan unionsrätten eller nationell rätt föreskriva och specificera vilka uppgifter och för vilka syften ytterligare personuppgiftsbehandling får ske. Om personuppgiftsbehandlingen grundar sig på individens samtycke, unionsrätt eller nationell rätt som utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle i syfte att säkerställa viktiga mål av allmänt intresse, bör personuppgiftsbehandling få ske ytterligare oavsett om det är förenligt med det ursprungliga ändamålet eller inte. Om en personuppgiftsansvarig som ett resultat av personuppgiftsbehandlingen överför uppgifter till en myndighet med anledning av misstänkt hot eller brott mot den allmänna säkerheten, ska detta beaktas som ett agerande av berättigat intresse.[71]

Personuppgifter som till sin natur är känsliga med beaktande av grundläggande fri- och rättigheter är som huvudregel förbjudna att behandla. Personuppgifter av detta slag är till exempel ras, etniskt ursprung, politisk tillhörighet och sexuell läggning, vilka bör åtnjuta ett särskilt skydd. [72]

[69] Art. 6 och skäl 19 GDPR.
[70] Skäl 19 2 st GDPR.
[71] Art. 6.4 och skäl 50 GDPR.
[72] Art 9.1 GDPR.

Eventuella undantag från sådant skydd bör uttryckligen anges i lag och omfattas av särskilda skyddsåtgärder för att tillvarata individens grundläggande rättigheter.[73] Personuppgifter som rör fällande domar i brottmål samt överträdelser eller till dessa sammanhängande säkerhetsåtgärder regleras genom art. 10 i GDPR. Sådana personuppgifter får endast behandlas under kontroll av en myndighet eller då behandlingen är tillåten genom gemenskapsrätt eller nationell rätt. Det förutsätter att lämpliga skyddsåtgärder för individens rättigheter vidtas.[74] Det ankommer den personuppgiftsansvarige att visa att de tvingande berättigande intressena väger tyngre än individens intressen och grundläggande fri- och rättigheter.[75]

3.5.2 Nödvändighet

Nödvändighetskravet är inte definierat i GDPR och är därmed något oklart. Att behandla personuppgifter förmodas vara nödvändigt för att nå ett ändamål, om ändamålet inte kan nås på annat sätt.[76] Det har dock ansetts orimligt att det skulle föreligga ett krav på omöjlighet att nå ett ändamål för att lagligen behandla personuppgifter. Istället har en påtaglig förenkling för att nå ändamålet ansetts tillräcklig för att lagligen behandla personuppgifter.[77] Nödvändighetskravet prövades i mål C-524/06 *Heinz Huber v Bundesrepublik Deutschland*.[78] Målet avsåg ett register upprättat av en tysk myndighet innehållandes personuppgifter om invandrade EU-medborgare till Tyskland, med syftet att tillgängliggöra informationen för samtliga myndigheter och därmed effektivisera myndighetsarbetet. Domstolen konstaterade att begreppet inte ska tolkas olika från medlemsstat till medlemsstat, utan ska tolkas självständigt gemenskapsrättsligt.[79] Domstolen konstaterade vidare att nödvändigheten är uppfylld om behandlingen av personuppgifterna uteslutande är sådana uppgifter som behövs för att kunna tillämpa bestämmelserna inom aktuellt verksamhetsområde, och att

[73] Art. 9.2, skäl 51 och 52 GDPR.
[74] Art. 10 GDPR.
[75] Skäl 69 GDPR.
[76] SOU 1999:109, s. 156.
[77] SOU 2001:32, s. 95; SOU 2001:100, s. 90.
[78] Domstolens dom (stora avdelningen) den 16 december 2008, ECLI:EU:C:2008:724.
[79] C-524/06 *Heinz Huber v Bundesrepublik Deutschland*, p. 52.

behandlingens karaktär på effektivt sätt uppfyller ändamålet.[80] Domstolen pekade även på att bekämpning av kriminalitet i sig är ett legitimt syfte för att behandla personuppgifter. Personuppgiftsbehandlingen i det aktuella fallet bedömdes dock inte vara godtagbar i ljuset av diskrimineringslagstiftning.[81]

3.5.3 Avtal

Art. 6.1 b innebär att behandling av personuppgifter får ske utan individens samtycke om behandlingen är nödvändig för att fullgöra ett avtal mellan avtalsparterna, eller på begäran av den registrerade vidta åtgärder innan sådant avtal ingås. Enligt den svenska översättningen av bestämmelsen krävs det att personen vars uppgifter som ska behandlas själv är avtalspart och inte bara berättigad enligt ett tredjemansavtal. Sören Öman framhåller att ett avtal mellan en personuppgiftsansvarig och en juridisk person därmed inte utgör en grund för laglig behandling av personuppgifter avseende den juridiska personens anställda. Vad gäller en individs begäran att en personuppgiftsansvarig ska behandla dennes personuppgifter avses till exempel begäran om kreditupplysning, offerter och uppgifter om lagfart.[82]

Avtal där individen vars personuppgifter ska behandlas är part, det vill säga när individen har givit sitt samtycke på ett eller annat sätt, är en rättslig förpliktelse som utgör en separat rättslig grund för personuppgiftsbehandlingen.[83]

3.5.4 Rättslig förpliktelse

Art. 6. 1 c och e reglerar personuppgiftsbehandling som grundar sig på en rättslig förpliktelse för en personuppgiftsansvarig respektive personuppgiftsbehandling som krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. För att lagligen behandla dessa typer av personuppgifter krävs en grund i EU-rätten eller den nationella

[80] C-524/06 *Heinz Huber v Bundesrepublik Deutschland,* p. 66.
[81] Ibid, p. 77.
[82] Öman, s. 153 ff.
[83] SOU 1997:39, s. 363; Art. 6. GDPR.

rätten.[84] Med nationell rätt avses den nationella rätt i den medlemsstat som verksamheten i fråga omfattas av.[85] Både svenska och EU-rättsliga utredningar inför GDPR lyfter att en personuppgiftsansvarigs skyldighet att behandla personuppgifter enligt tredje lands lag inte utgör en rättslig förpliktelse i den bemärkelse som avses i GDPR. En personuppgiftsansvarig är därmed förhindrad att på rättslig grund behandla personuppgifter med hänvisning till tredje lands lag, även om personuppgiftsbehandlingen är nödvändig för att uppfylla förpliktelsen enligt tredje lands lag.[86] Artikel 29-gruppen framhåller att sådan reglering dock kan utgöra en rättslig förpliktelse genom mellanstatliga avtal mellan aktuell medlemsstat och tredje land. Fullgörelse av en rättslig förpliktelse i tredje land kan dessutom ligga i den personuppgiftsansvarigas intresse i enlighet med art. 6.1 f. Vidare konstaterar Artikel 29-gruppen att en rättslig förpliktelse inte omfattar situationer när personuppgiftsansvariga har valfrihet att följa den rättsliga förpliktelsen. Som exempel på när bestämmelsen om rättslig förpliktelse inte är tillämplig anges en internetleverantörs ansträngningar att utan tydlig och specifik skyldighet i lag övervaka användarnas sökningar för att förhindra illegala nedladdningar.[87]

För att lagligt behandla personuppgifter med hänvisning till rättslig förpliktelse, krävs att den rättsliga förpliktelsens syfte med personuppgiftsbehandlingen framgår. En rättslig förpliktelse anses därmed inte utgöra en rättslig grund för behandlingen om förpliktelsen är alltför svepande och ger den personuppgiftsansvariga för stort handlingsutrymme för kravens uppfyllnad. Artikel 29-gruppen tycks mena att graden av specificering kan variera utifrån förpliktelsens nivå i normhierarkin. Bindande myndighetsbeslut och sekundära rättskällor bör innehålla desto mer specificerade och konkretiserade rättsliga förpliktelser. Vidare konstaterar Artikel 29-gruppen att situationer då myndigheter publicerar generella riktlinjer och villkor som kan leda till sanktioner utfärdat av samma

[84] Art. 6.3 och skäl 45 GDPR.
[85] Art. 6.3 b GDPR.
[86] SOU 2017:39, s. 110; D-post: BRYR/2016-05-01/1503; Artikel 29-gruppens yttrande 6/2014, s. 19.
[87] Artikel 29-gruppens yttrande 6/2014, s. 19.

myndighet, till exempel regulatoriska riktlinjer om särskilda standarder för *due diligence* till finansiella institut, istället bör bedömas under art. 6.1 f som ett berättigat intresse i balanserande syfte.[88] Inför den svenska kompletteringen diskuterades hur en rättslig grund bör utformas. Förslaget landade i att lagregleringen inte behöver avse själva behandlingen av personuppgifter, utan istället reglera den rättsliga förpliktelse som avses eller det allmänna intresset som ska tillgodoses. Detta kan genomföras genom författningar eller meddelade beslut i enlighet med regeringsformen.[89]

I förarbeten påpekas vidare att en rättslig förpliktelse rent språkligt omfattar även annan av rättsordningen erkänd ordning. Den svenska arbetsmarknadsmodellen medför att rättsliga förpliktelser och uppgifter av allmänt intresse kan följa av kollektivavtal.[90] Att kollektivavtal utgör en rättslig förpliktelse framgår även av 2 kap. 1 dataskyddslagen. Remissinstanser som Datainspektionen, Dataskydd.net och Srf konsulternas förbund motsatte sig en sådan struktur, med påpekandet att kollektivavtal inte är allmänt giltiga. Datainspektionen uttryckte i sitt remissvar en risk för att personuppgiftsbehandlingen inte kan utföras av behöriga aktörer med samhällsviktiga funktioner om det inte uttryckligen säkerställs genom nationell lagstiftning där behov finns. Datainspektionen anförde också att det skulle innebära att den personuppgiftsansvariga själv måste göra bedömningen om den rättsliga förpliktelsen lever upp till kraven i art. 6.3.

Vad gäller frågan om kollektivavtal ställde sig remissinstanser som Arbetsgivarverket, Landsorganisationen i Sverige och Collectum positiva till möjligheten att reglera frågan i kollektivavtal.[91] Sören Öman framhåller att Datainspektionen tycks vara av uppfattningen att bestämmelser i kollektivavtal mellan organisationer, arbetsgivare och fackföreningar kan i de delar som anses flyta samman med det individuella anställningsavtalet utgöra en grund för kollektivavtalsparterna att behandla personuppgifter.[92]

[88] Artikel 29-gruppens yttrande 6/2014, s. 19 ff.
[89] Prop. 2017/18:105, s. 49.
[90] Ibid, s. 48.
[91] Ibid, s. 48 f.
[92] Öman, s. 155 ff.

Situationen tycks då omfattas av art. 6.1 b som innebär att behandling av personuppgifter får ske utan individens samtycke om behandlingen är nödvändig för att fullgöra ett avtal mellan de två parterna.

Vad gäller den rättsliga förpliktelsens specificering menade regeringen i utredningen att en personuppgiftsansvarig kan förlita sig på att svensk rätt lever upp till samtliga principer och krav, med anledning av EKMR.[93] En personuppgiftsbehandling måste bedömas från fall till fall utifrån personuppgiftsbehandlingens och verksamhetens karaktär. En mer kännbar personuppgiftsbehandling som till exempel inom hälso- och sjukvården kräver en mer specificerad reglering, än vad till exempel hantering av elevers namn i en skolas vardagliga verksamhet gör. Om en personuppgiftsbehandling utgör ytterligare intrång som innebär övervakning eller kartläggning av en individs personliga förhållanden krävs det lagstöd enligt 2 kap. 6 och 20 §§ regeringsformen. 2 kap. 6 § 2 st. regeringsformen stadgar att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.[94]

Öman påpekar att det vid bedömning av om en rättslig förpliktelse föreligger eller ej inte bara följer av en uttrycklig lagregel, utan även förarbeten, bestämmelsens syften och den rättsliga kontexten kan behöva beaktas. Den rättsliga förpliktelsen kan även ha sin grund genom rättsligt reglerade avtal, som till exempel försäkringsavtal och kollektivavtal. Det kan genom lag föreskrivas att vissa typer av avtal måste ges ett visst innehåll, innebärande att personuppgiftsbehandling kan utgöra en förutsättning för att uppfylla lagkravet.[95]

3.5.5 Nödvändigt för berättigade intressen

Enligt GDPR art. 6.1 d-f anses personuppgiftsbehandling laglig när behandlingen kan tjäna intressen som är av grundläggande betydelse för

[93] Prop. 2017/18:105, s. 50.
[94] Ibid, s. 51.
[95] Öman, s. 158 ff.

individen vars personuppgifter behandlas eller annan fysisk person, om personuppgiftsbehandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning samt slutligen om personuppgiftsbehandlingen är nödvändig för ändamål som rör den personuppgiftsansvarigas eller tredje parts berättigade intressen. Av relevans i detta sammanhang är de två sistnämnda punkterna e och f.

Exempel på vad Datainspektionen har ansett utgöra personuppgiftsbehandling av berättigat intresse är ett närvarosystem hos ett byggföretag, där obligatorisk närvaro- och ID-registrering lagrades i två år för att möjliggöra informationsutlämning till Skatteverket för skattekontroll.[96] Vad gäller personuppgiftsbehandling i tredje parts intresse så exemplifierar Öman fall då personuppgifter behandlas med avsikt att upptäcka om den aktuella individen begår bedrägeri mot en annan enskild person.[97]

3.5.5.1 Allmänt intresse

Art. 6.1 e fastställer att personuppgifter får behandlas utan samtycke om behandlingen anses nödvändig för att utföra en arbetsuppgift av allmänt intresse eller vid myndighetsutövning och om det finns laga grund för behandlingen genom EU-rätt eller nationell rätt. Öman konstaterar att det är oklart om bestämmelsen avser nödvändig behandling i direkt anslutning till myndighetsutövning eller om det avser personuppgiftsbehandling för arbetsuppgifter som ett led i myndighetsutövningen.[98] Öman ställer sig frågande till kollektivavtal i detta hänseende, då det genom 2 kap. 1 § dataskyddslagen framgår att en arbetsuppgift av allmänt intresse även kan framgå av kollektivavtal. Hur vidsträckt betydelse ett kollektivavtal kan få eller under vilka omständigheter framgår inte.[99]

Vad som utgör ett allmänt intresse definieras inte i GDPR. Situationer som hälso- och sjukvård, socialt skydd och arkivändamål exemplifieras dock

[96] Datainspektionens yttrande 2007-05-25, dnr 1036–2006.
[97] Öman, s. 173 f.
[98] Ibid, s. 162 f.
[99] Ibid, s. 165 ff.

under olika delar som allmänna intressen.[100] Regeringen har uttryckt olika tolkningar av begreppet, dels att begreppet måste ges en vid betydelse för att myndigheternas verksamhet ska kunna fungera, dels att ett allmänt intresse är sådan verksamhet som ska finnas i enlighet med internationella rättighetsstadgor.[101]

En arbetsuppgift av allmänt intresse förutsätter inte att arbetsuppgiften måste utföras. En kommun bedrivs visserligen med syfte till det allmänna intresset, men viss verksamhet inom kommunen är frivillig, till exempel idrottsverksamhet, åtgärder för att främja näringsliv och tillhandahålla kultur annat än genom bibliotek. Privata aktörer kan utföra arbetsuppgifter av allmänt intresse på uppdrag av myndighet eller på eget initiativ. Bedömningen om en arbetsuppgift är av allmänt intresse bör göras mot bakgrund av verksamhetens syfte, till exempel förskoleverksamhet, rikstäckande infrastruktur och energiförsörjning. Öman konstaterar att flera av de privata verksamheter som anses utföra arbetsuppgifter av allmänt intresse är lagreglerade, innebärande att inte enbart själva arbetsuppgiften av allmänt intresse är lagreglerad, utan även verksamheten som sådan.[102] Arbetsuppgifter av allmänt intresse har även ansetts vara myndigheters utlämnande av information för användning i kreditupplysningsverksamhet och att i samband med kreditupplysning förmedla uppgifter om ekonomisk brottslighet, i syfte att ge näringsidkare bättre skydd mot ekonomisk brottslighet.[103] Datainspektionen har däremot i ett beslut konstaterat att ett statligt spelbolags kartläggning av spelbeteende för att upptäcka beroende- och spelmissbruk inte var nödvändigt för att utföra en arbetsuppgift av allmänt intresse.[104]

3.5.5.2 Personuppgiftsansvariges intresse

Art. 6.1 f innebär att en personuppgiftsansvarigs eller tredje parts berättigade intressen kan utgöra en rättslig grund för personuppgiftsbehandling, under

[100] Art. 5.1 b, skäl 45, 52–56, 112 och 154 GDPR.
[101] Prop. 2017/18:105, s. 56; SOU 2017:66, s. 219 ff.
[102] Öman, s. 166 ff.
[103] Prop. 2017/18:95, s. 44 f; Prop. 2000/01:105, s. 36.
[104] Öman, s. 168 f*;* Datainspektionens beslut 2015-10-15, dnr 1382–2014.

förutsättning att den enskilda individens intressen eller grundläggande rättigheter inte väger tyngre med beaktande av dennes förväntningar till följd av förhållandet till den personuppgiftsansvarige. Öman konstaterar att bestämmelsen är en generalklausul och fungerar som en säkerhetsventil i de situationer de tidigare punkterna inte kan tillämpas. Öman tycks i övrigt ställa sig mycket frågande till hur en dylik intresseavvägning ska utföras.[105]

Ett intresse kan vara berättigat både från ett allmänneligt perspektiv och ett mer individualiserat perspektiv. Det innebär att det berättigande av ett intresse varierar beroende på vilken situation som ligger för handen.[106] I skälen till GDPR anges ett berättigande intresse till exempel vara när det redan föreligger ett förhållande mellan individen och den personuppgiftsansvarige genom till exempel en kundtjänst eller anställning. Ett berättigat intresse ställer krav på noggrann bedömning, inklusive bedömningen om individen rimligen kan förvänta sig att personuppgiftsbehandlingen kan komma att användas till det aktuella ändamålet. Om det framstår som orimligt att individen skulle kunna förvänta sig en viss behandling av uppgifterna, väger individens intressen tyngre än den personuppgiftsansvariges intressen. Skälen påpekar särskilt att behandling av personuppgifter som är nödvändig för att förhindra bedrägerier utgör ett berättigat intresse.[107] Öman menar att även intressen som är fastslagna genom internationella rättighetsstadgor inom EU utan tvekan bör anses utgöra berättigade intressen som väger tungt i avvägningen. Artikel 29-gruppen exemplifierar utövande av informations- och yttrandefrihet, konventionell direkt marknadsföring, icke begärda kommersiella meddelanden inklusive politiska kampanjer, verkställande och indrivning av rättsliga krav, förhindrande av bedrägeri, missbruk eller penningtvätt och visselblåsarsystem som berättigande intressen. För att anses som ett berättigande intresse måste intresset vara godtagbart enligt lag samt utgöra ett reellt intresse, det vill säga inte ett spekulativt intresse.[108]

[105] Öman, s. 170 f.
[106] Artikel 29-gruppens yttrande 6/2014, s. 24.
[107] Skäl 47 GDPR.
[108] Artikel 29-gruppens yttrande 6/2014, s. 25.

3.5.5.3 Balanstest

Artikel 29-gruppen menar att enbart ett legitimt intresse inte räcker för att en personuppgiftsbehandling ska anses tillåten under art. 6.1 f, utan det krävs även att ett ”balanstest” utförs. Balanstestet ska innehålla bedömningar avseende den personuppgiftsansvariges legitima intressen, påverkan på individen, preliminär åtgärdsbalans och ytterligare säkerhetsåtgärder för att förhindra otillbörlig påverkan på individen.[109]

Personuppgiftsansvariges legitima intressen

För att reglers legitima intresse ska anses föreligga som grund för behandling, måste databehandlingen vara nödvändig och proportionell för att utöva den grundläggande rättigheten. Som exempel anför Artikel 29-gruppen att det å ena sidan kan vara nödvändigt och proportionerligt för en tidning att publicera vissa inkriminerande ekonomiska uppgifter om en tjänsteman på hög nivå vid en påstådd korruptionsskandal. Å andra sidan bör det inte finnas något tillstånd för media att publicera övriga irrelevanta uppgifter om tjänstemannens privatliv. Dylika fall utgör vanligtvis komplexa bedömningsfrågor och till hjälp för bedömningen kan specifik lagstiftning, rättspraxis, riktlinjer, uppförandekoder och andra formella eller mindre formella standarder användas. När det är lämpligt kan även ytterligare skyddsåtgärder vara till hjälp i bedömningsfrågan.[110]

I vissa fall kan den personuppgiftsansvariga önska att åberopa allmänintresset eller intresset hos det stora samhället, oavsett om det föreskrivs i nationella lagar eller förordningar. En välgörenhetsorganisation kan till exempel behandla personuppgifter för medicinsk forskning och en ideell organisation för att öka medvetenheten om regeringens korruption. Det kan också vara så att ett privat företagsintresse hänger samman med ett allmänt intresse, till exempel vid bekämpning av ekonomiskt bedrägeri eller annat bedrägligt användande av tjänster. En tjänsteleverantör kan ha ett legitimt affärsintresse att försäkra sig att kunderna inte missbrukar tjänsten eller inte kommer få betalt för tjänsten, samtidigt som kunderna i företaget, skattebetalarna och

[109] Artikel 29-gruppens yttrande 6/2014, s. 33.
[110] Ibid s. 34 f.

allmänheten i stort också har ett legitimt intresse att se till att bedrägliga aktiviteter förebyggs och upptäcks. Generellt kan det faktum att en personuppgiftsansvarig inte bara verkar i sitt egna legitima intresse utan också för det bredare samhällets intresse ge större vikt åt det intresset. Ju mer övertygande och erkänt allmänintresset eller intresset hos det bredare samhället är, desto starkare väger intresset i bedömningen. Samhället och individen förväntar sig då att den personuppgiftsansvarige kan vidta åtgärder och behandla personuppgifter i strävan efter dessa intressen. Däremot bör "privat verkställighet" av lagen inte användas för att legitimera påträngande metoder som, om de genomförs av en statlig organisation, är förbjudna att vidta för offentliga organ enligt rättspraxis från Europeiska domstolen för de mänskliga rättigheterna.[111]

I vissa fall kan intressen sammanfalla med de i art. 6 angivna lagliga behandlingsgrunderna, men lämpa sig bättre att ta hänsyn till i balanstestet. Det kan till exempel vara fråga om en rättslig förpliktelse som får men inte måste utföras eller en personuppgiftsbehandling som inte är direkt nödvändig men ändock relevant för genomförandet av ett kontrakt.[112]

Existensen av vägledande och icke-bindande dokument utfärdade av till exempel myndigheter som bidrar till att nå ett visst mål med ett intresse är av betydelse för bedömningen av en personuppgiftsbehandling. Efterlevnad av sådan vägledning kan bidra till intresseavvägningen till fördel för den personuppgiftsansvarige. Kulturella och sociala förväntningar spelar också roll i avvägningen, även om förväntningarna inte återspeglas direkt genom lag.[113]

Påverkan av individen

Påverkansbedömningen ska ta hänsyn till positiva och negativa konsekvenser som kan följa av personuppgiftsbehandlingen för den enskilda individen, som till exempel risker för diskriminering, anseende, förhandlingsposition och självständighet. Hänsyn ska också tas till den rädsla och stress som individen

[111] Artikel 29-gruppens yttrande 6/2014, s. 35.
[112] Ibid, s. 35 f.
[113] Ibid, s. 36.

kan utsättas för genom att förlora kontroll över sina personuppgifter, som till exempel kan ske genom internetexponering. Till bedömningen kommer också hur pass allvarlig en eventuell konsekvens kan komma att bli.[114]

Vid bedömning ska hänsyn tas till hur känslig karaktär personuppgifterna har. Ju känsligare personuppgifter kan konstateras vara, desto större konsekvenser kan behandlingen få för individen. Med det sagt så innebär det inte att oskadliga personuppgifter får användas fritt under bestämmelsen, då uppgifter som framstår som obetydliga ändå kan få signifikanta konsekvenser för den enskilde. Vid bedömningen är det av relevans huruvida individen själv har gjort uppgifterna offentligt tillgängliga på eget initiativ eller ej, särskilt om uppgifterna har gjorts tillgängliga under omständigheter relaterade syften att tillförse transparens och ansvar.[115]

Vid bedömning av behandlingsprocessen ska hänsyn tas till huruvida personuppgifterna på ett eller annat sätt kommer att vara tillgängligt för en större publik eller om personuppgifterna kommer att behandlas tillsammans med annan data. Detta kan ske till exempel vid profilering i olika sammanhang. Behandling av personuppgifter kan i sådana fall leda till besynnerliga, oväntade och oriktiga konsekvenser för individen. Ju mer osäker och negativ en personuppgiftsbehandling är, desto större är risken att behandlingen inte är att anse som legitim.[116]

Hänsyn ska tas till vilka rimliga förväntningar individen kan ha i förhållande till användning och exponering av dennes personuppgifter. I detta avseende kan det vara av relevans att beakta andra omständigheter där det kan anses påkallat att personuppgifterna behandlas.[117]

Maktförhållandet mellan den personuppgiftsansvarige och individen kan också vara av relevans för bedömningen. En personuppgiftsansvarig som är mer eller mindre dominant på marknaden eller är ett multinationellt företag

[114] Artikel 29-gruppens yttrande 6/2014, s. 37 f.
[115] Ibid, s. 38 f.
[116] Ibid, s. 39 f.
[117] Ibid, s. 40.

har mer resurser och förhandlingsutrymme att argumentera för sitt berättigade intresse än den enskilda individen. Av relevans är också om den enskilda individen till exempel är ett barn eller tillhör en grupp som behöver extra skydd, till exempel psykiskt sjuka, asylsökande och äldre människor. Vad den personuppgiftsansvarige och individen har för relation sinsemellan är också relevant för bedömningen av maktbalansen, till exempel under anställningsförhållanden.[118]

Åtgärdsbalans

Vid balansbedömningen ska samtliga principer i direktivet beaktas. Det innebär att balansbedömningen som görs under aktuell bestämmelse till stor del vilar på huruvida den personuppgiftsansvarige utför och upprätthåller den regelefterlevnad som direktivet kräver. Regelefterlevnad innebär dock inte en garanti för tillräcklig legal grund under aktuell bestämmelse. I de fall det är svårt att göra balansavvägningen kan ytterligare skyddsåtgärder anses påkallat, till exempel upprättande av ett mekaniskt verktyg som underlättar för individen att avlägsna sina personuppgifter.[119]

Ytterligare säkerhetsåtgärder

Desto större påverkan personuppgiftsbehandlingen får för den enskilda individen, desto mer uppmärksamhet till skyddsåtgärder krävs. Åtgärder som kan balansera behandlingen till den personuppgiftsansvariges intressen är till exempel restriktivitet kring hur mycket personuppgiftsdata som får inhämtas och omedelbar radering av personuppgifter efter behandling. Trots att vissa åtgärder är obligatoriska för personuppgiftsansvariga finns det alltid utrymme för extra skyddsåtgärder.[120]

3.5.6 Känsliga uppgifter

Art. 9 förbjuder som huvudregel behandling av personuppgifter som avslöjar känsliga uppgifter som till exempel etniskt ursprung, politiska åsikter, religiösa övertygelser och genetiska uppgifter. Undantag från förbudet kan

[118] Artikel 29-gruppens yttrande 6/2014, s. 40 f.
[119] Ibid, s. 41.
[120] Ibid, s. 42.

göras genom samtycke, såtillvida samtycke till behandling av känsliga uppgifter inte är förbjudet enligt unionsrätten eller nationell rätt.[121] Vidare får känsliga personuppgifter behandlas om det bland annat krävs för att fullgöra skyldigheter och rättigheter inom områdena för arbetsrätt eller hälso- och socialomsorg vilka har stöd i unionsrätten, nationella rätten eller kollektivavtal, eller om behandling är nödvändig med hänsyn till ett viktigt allmänt intresse.[122] Vid behandling av känsliga uppgifter måste den personuppgiftsansvariga göra en konsekvensbedömning i enlighet med art. 35.3 b, om behandlingen är att anse som omfattande.[123]

Enligt dataskyddslagen får personuppgifter behandlas av om behandlingen är nödvändig för fullgörande av skyldigheter och rättigheter inom arbetsrätt och social trygghet och skydd. Sådana uppgifter får endast lämnas ut till tredje part om det finns en skyldighet inom nämnda rättsliga områden att lämna ut personuppgifterna.[124]

Begreppet allmänt intresse i art. 9.2 g har i denna bestämmelse samma innebörd som tidigare anfört om allmänt intresse under art. 6.1. Begreppet används även i art. 17 avseende folkhälsoområdet samt art. 23.1 e vilken tar sikte på samhällets viktiga ekonomiska eller finansiella intressen, som till exempel penning- budget- och skattefrågor, folkhälsa och social trygghet. När känsliga personuppgifter ska behandlas i enlighet med ett viktigt allmänt intresse krävs ett rättsligt stöd i enlighet med art. 6.1 c och e, innebärande att en rättslig förpliktelse, arbetsuppgift eller myndighetsutövning som den känsliga personuppgiftsbehandlingen är nödvändig för måste ha stöd i unionsrätten eller den nationella rätten.[125] I Sverige har verksamhet av viktigt allmänt intresse ansetts vara sådan som innefattar myndighetsutövning, medan kreditupplysningsverksamhet inte har ansetts utgöra detsamma.[126] Således får endast myndigheter behandla känsliga personuppgifter med stöd

[121] Art. 9.2 a GDPR.
[122] Art. 9.2 b och g GDPR.
[123] Öman, s. 226.
[124] 3 kap. 2 § dataskyddslagen.
[125] Öman, s. 249 ff
[126] Prop. 2017/18:105, s. 83; Prop. 2000/01:50, s. 23.

av bestämmelsen viktigt allmänt intresse, om inte regeringen meddelar annat genom föreskrift.[127]

Avseende kategorin *politisk åsikt* bör uppgifter om medlemskap i och bidrag till politiska partier enligt förarbeten räknas som politisk åsikt, vilket innebär att uppgifter om politiska bidragsgivare är att anse som känsliga.[128]

Monika Wendleby och Dag Wetterberg framhåller att det inte är helt enkelt att förstå vilka undantag i GDPR som kräver kompletterande nationell lag och vilka undantag som är direkt tillämpliga. Frågan måste avgöras genom framtida praxis.[129]

3.5.7 Brottsuppgifter

Art. 10 behandlar personuppgifter som rör fällande domar och brottsöverträdelser. Behandling av sådana personuppgifter får endast utföras under kontroll av behörig myndighet eller om behandling med lämpliga säkerhetsåtgärder tillåts genom unionsrätt eller nationell rätt. Behandlingen ska i tillägg ska ha en rättslig grund i enlighet med art. 6.1.[130] Behandling av brottsuppgifter får enligt Datainspektionen dock inte utföras med individens samtycke som grund.[131] Något principiellt förbud mot behandling av brottsuppgifter, likt förbudet mot behandling av känsliga personuppgifter, finns dock inte i GDPR.[132]

Vid överföring av personuppgifterna till tredjeland eller en internationell organisation måste även art. 44–50 följas, vilka föreskriver ytterligare säkerhetsåtgärder. Vid behandling av brottsuppgifter måste den personuppgiftsansvariga även göra en konsekvensbedömning i enlighet med art. 35.3 b, om behandlingen är att anse som omfattande.[133] Öman framhåller att det är oklart i vilken utsträckning bestämmelsen omfattar lagöverträdelser

[127] 3 kap. 3 och 4 §§ dataskyddslagen.
[128] Ds 2013:31, s. 115 f; Prop. 2013/14:70, s. 74.
[129] Wendleby & Wetterberg, s. 90 ff.
[130] Öman, s. 260 ff.
[131] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/, besökt 2019-08-07.
[132] Prop. 2017/18:105, s. 99.
[133] Öman, s. 260 f.

som innefattar brott enligt utländsk lagstiftning, men att bestämmelsen kan antas innebära att personuppgifter som rör ett straffbart förfarande i tredjeland men icke straffbart i en medlemsstat, inte omfattas.[134] Det står inte heller klart vad som krävs för att personuppgiftsbehandling ska anses ske under kontroll av en myndighet. Öman konstaterar att det dock i bestämmelsens mening inte är tillräckligt med en tillsynsmyndighet som övervakar tillämpningen av GDPR och har omfattande befogenheter.[135]

Brottsuppgifter får enligt förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddsförordningen) behandlas av andra än myndigheter om behandlingen är nödvändig för att göra gällande, fastställa eller försvara rättsliga anspråk eller för fullgörande av en rättslig förpliktelse enligt lag eller förordning. Datainspektionen får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som avses i GDPR art. 10, samt i enskilda fall besluta att andra än myndigheter får behandla sådana personuppgifter.[136]

Datainspektionen får även meddela tillstånd att brottsuppgifter behandlas i kreditupplysningsverksamhet, om synnerliga skäl föreligger.[137] Datainspektionen har meddelat att behandling av brottsuppgifter av annan aktör än myndighet får ske om det är nödvändigt för att fullgöra uppgifter inom socialtjänstområdet, om behandlingen avser anteckningar i fristående skolors och högskolors elevvårdande verksamhet, för att kontrollera jävssituationer inom advokatverksamhet samt om personuppgiftsbehandlingen avser personer i ledande ställning eller nyckelpositioner inom det egna bolaget eller koncernen i inrättade visselblåsarsystem i syfte att upptäcka och utreda allvarliga oegentligheter. Exempel på allvarliga oegentligheter är om det rör bokföring, intern bokföringskontroll, revision, mutor, brottslighet inom bank- och finansväsen

[134] Öman, s. 266.
[135] Ibid, s. 269 f.
[136] 5–6 §§ dataskyddsförordningen.
[137] Prop. 2000/01:50, s. 23 f.

eller andra allvarliga omständigheter som rör organisationens vitala intressen eller enskildas liv och hälsa.[138]

Förarbeten ger uttryck för tillåtlig personuppgiftsbehandling avseende brottsöverträdelser när det gäller bland annat forskning och arkivändamål av allmänt intresse.[139] I utredningen inför dataskyddslagen påpekas att rättsliga förpliktelser av personuppgiftsbehandling avseende lagöverträdelser kan förekomma i reglering som syftar till att bekämpa till exempel korruption, terrorism, finansiering av grov brottslighet och olämplig spridning av vapenteknologi. Det ansågs dock inte ligga inom uppdragets ramar att utreda vilka rättsliga förpliktelser som redan fanns och därmed stod i strid med GDPR, men att en normkonflikt skulle vara problematisk.[140] Utredningen tog enbart sikte på de konsekvenser som kunde uppstå genom de förändringar som GDPR innebar i förhållande till dåvarande personuppgiftslagen och personuppgiftsförordningen.[141] Slutsatsen av utredningen var att inga nya ekonomiska eller administrativa konsekvenser i negativ riktning skulle uppstå, utan enbart konsekvenser i positiv riktning för enskildas integritetsskydd samt minska antalet kriminaliserade handlingar.[142]

Utredningen poängterar också att art. 10 i GDPR inte ger stöd för ett förbud för andra aktörer än myndigheter att behandla uppgifter gällande administrativa frihetsberövanden, men att sådan behandling ändå kan omfattas av förbudet att behandla känsliga uppgifter i art. 9.1 samt att art. 5 om principer för personuppgiftsbehandling och art. 6 om laglig personuppgiftsbehandling rent praktiskt torde innebära begränsande möjligheter för privata aktörer att behandla sådana uppgifter.[143]

[138] 2 § DIFS 2018:2.
[139] SOU 2017:39, s. 23.
[140] Ibid, s. 195.
[141] SOU 2017:39, s. 349; Kommittédirektiv 2016:15, s. 14 ff.
[142] SOU 2017:39, s. 349.
[143] Ibid, s. 195.

4 Tredjepartsbesiktning som rättslig förpliktelse

4.1 Sverige

I 10 kap. 5 e § brottsbalken (BrB) regleras vårdslös finansiering av mutbrott, vilken kan konstateras vara den reglering som ligger närmast ett undersökningskrav av affärspartners. Bestämmelsen innebär att en näringsidkare eller verksamhetens verkställande ledning som tillhandahåller pengar eller andra tillgångar åt någon som företräder näringsidkaren i en viss angelägenhet och därigenom av grov oaktsamhet främjar givande av muta, grovt givande av muta eller handel med inflytande döms till böter eller fängelse upp till två år. Verksamheten kan även åläggas företagsbot på upp till 10 miljoner kronor, om näringsidkaren inte har gjort vad som skäligen kan krävas för att förebygga brottsligheten eller brottet har begåtts av någon i en ledande ställning inom företaget eller som annars har ett särskilt ansvar för tillsyn och kontroll.[144] Främjandet ska innefatta ett kvalificerat otillåtet risktagande, vilket till exempel kan vara att inte vidta tillräckliga kontroll- eller försiktighetsåtgärder avseende företrädaren som i denna egenskap förses med tillgångar.[145]

I remissvar till utredningen anförde Åklagarmyndigheten att bestämmelsens konstruktion förutsätter att mutbrotten har utförts eller kommer att utföras, utan att näringsidkaren rent straffrättsligt är medveten om det. Vidare ifrågasatte Åklagarmyndigheten varför bestämmelsen kräver ett styrkt mutbrott, eftersom det är just den bristande kontrollen vid erbjudandet, utlovandet och lämnandet av medlen som kriminaliseras. När mutbrottet begås har den vårdslösa näringsidkaren redan begått den straffvärda handlingen, nämligen i det ögonblick denne erbjöd, utlovade eller lämnade medel till mellanmannen. Vidare menade Åklagarmyndigheten att mutbrottets fullbordande i sådana situationer är rena tillfälligheter som ligger

[144] 36 kap. 8 § BrB.
[145] Friberg, not. 558.

helt utanför den aktuella näringsidkarens egentliga kontroll. Om näringsidkaren har skaffat sig kännedom om begånget mutbrott, så har denne istället gjort sig skyldig till just mutbrott. Åklagarmyndigheten ansåg att brottet skulle konstrueras så att den straffbara handlingen anknyts till näringsidkarens bristande kontroll av mellanmannen, och därmed inneburit ett främjande av fara eller allvarlig fara för brott.[146]

Ekobrottsmyndigheten anförde kritik i samma riktning som Åklagarmyndigheten, nämligen att regelns struktur riskerar att bli svårtillämpad i praktiken, eftersom regeln går ut på att visa att finansieringen lett till att mutbrott har begåtts.[147] Istället ansågs det befogat att oaktsamheten skulle utgöra ett självständigt klandervärt beteende, och inte vara beroende av att mutbrott har genomförts.[148] Denna hållning intog inte regeringen av straffrättsliga förutsebarhetsskäl samt att en sådan reglering skulle ge uttryck för en alltför passiv syn på företagsledningens roll, vad gäller åsikten att det ligger utanför ledningens kontroll att överlämnade medel kom till användning av mellanmannens mutbrott. Istället ansågs den föreslagna bestämmelsen ge incitament för företagsledningen att utföra kontroller av mellanhänder.[149]

I propositionen till införandet av vårdslös finansiering av mutbrott anförs att Sverige genom anslutning till OECD, Europarådskonventionen och FN-konventionen åtagit sig att inte bara utforma straffansvar för korruptionsbrott, utan även upprättande av åtgärder i förbyggande syfte.[150] Genom ekonomiska sanktioner som företagsbot skapas, utöver straffbestämmelserna, incitament för företag att arbeta proaktivt för att förhindra förekomsten av korruption i den egna verksamheten. Vidare konstateras att det i en seriöst bedriven näringsverksamhet finns ett stort egenintresse att förhindra korruption, men att det utöver internationella och nationella uppförandekoder behövs ytterligare åtgärder för att på alla nivåer nå den ambition och potential som finns för att förebygga korruption. Det anses också vara ett straffvärt beteende

[146] Åklagarmyndighetens yttrande ÅM-A 2010/1097, s. 1.
[147] Prop. 2011/12:79, s. 35; Dnr Ju2010/4890/L5; Dnr EBM A-2010/0318.
[148] Prop. 2011/12:79, s. 37.
[149] Ibid, s. 37.
[150] Ibid, s. 35 f.

att strukturera sin näringsverksamhet på ett sådant vis att förebyggande åtgärder, som till exempel kontroll av verksamhetens företrädare, omöjliggörs.[151] En näringsidkare ska skaffa sig goda kunskaper om företrädaren och eventuella motparter som kan involveras i affären vid nyttjande av finansieringen och hur tillgångarna kan komma att användas. En högre kontrollnivå anses påkallat i de situationer då företrädaren är verksam i länder eller regioner där korruption kan sägas vara en vanlig företeelse. Det blir också av vikt för oaktsamhetsbedömningen huruvida tillräckliga instruktioner och rutiner har funnits på plats för att förhindra korrupt agerande. Sådana brister kan innebära att ledningen inte har gjort vad som skäligen kan krävas i det förebyggande arbetet mot mutbrott.[152] Cars understryker att ansvar kan undvikas genom att företa åtgärder som *due diligence* före anlitandet av företrädaren, och därmed undersöka företrädarens bakgrund och ekonomiska ställning.[153]

Vad gäller politiska partiers redovisningskrav intäkter så framgår detta av 3 § lag (2018:90) om insyn i finansiering av partier (Insynslagen). Lagen syftar bland annat till att motverka korruption.[154] Det konstateras i förarbeten att externa politiska bidrag är i riskzonen för korruption, varför det finns ett extra starkt allmänt intresse för öppenhet och insyn i vilka intressen som står bakom partiers finansiering.[155] Genom flertalet bestämmelser i insynslagen framgår att bidragsgivarens identitet måste registreras och redovisas för Kammarkollegiet, vilket omfattar uppgifter som namn, personnummer och adress.[156] I propositionen uppmärksammas att art. 9.2 g i GDPR principiellt förbjuder behandling av uppgifter som avslöjar politiska åsikter, men att behandlingen kan tillåtas om den nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt. Insyn i politiska partiers finansiering ansågs vara ett sådant allmänt intresse, och även uppfylla GDPR:s övriga grundläggande principer. Det innebär regeringen ansåg att GDPR gav rättsligt stöd för att de som ålades

[151] Prop. 2011/12:79, s. 36.
[152] Ibid, s. 50.
[153] Cars, s. 51.
[154] Prop. 2013/14:70, s. 111.
[155] Ds 2013:79, s. 115 f; Prop. 2013/14:70, s. 105.
[156] Se bland annat 2, 21 och 27 §§ insynslagen.

skyldigheter att redovisa finansieringen skulle kunna behandla uppgifter som avslöjar politiska åsikter. Det ansågs därför inte nödvändigt med en särskild bestämmelse i insynslagen avseende personuppgiftsbehandlingen.[157]

4.2 Irland

Number 7 of 2018 Data Protection Act 2018 tillåter uttryckligen reglering som innebär behandling av brottsuppgifter under nödvändiga och proportionerliga förhållanden i syfte att bedöma risker eller förhindra förekomsten av bestickning och korruption.[158] *Enligt Number 9 of 2018 Criminal Justice (Corruption Offences) Act 2018* är en verksamhet skyldig till brott om en tjänsteman, anställd, ombud eller dotterbolag till företaget har begått brottet, med syfte att erhålla eller behålla företag eller någon affärsfördel för företaget. Boten som kan ådömas verksamheten är obegränsad. I tillägg har personen som begår brottet samt verksamhetens ledning ett personligt straffansvar och kan dömas till fängelse upp till 10 år samt böter till ett obegränsat belopp.[159] Det anförda innebär att samma ogiltiga handling kan åtalas på tre olika fronter: verksamheten, den person som begått den olagliga handlingen och en tjänsteman i företaget som samtyckt till handlingen eller varit försumlig. Straffansvar kan undvikas om det kan visas att verksamheten vidtog skäliga åtgärder och utförde all undersökning för att förhindra att brottet begicks.[160]

[157] Prop. 2017/18:55, s. 94.
[158] Art. 55 (3)(b) Number 7 of 2018 Data Protection Act 2018.
[159] Section 17 Number 9 of 2018 Criminal Justice (Corruption Offences) Act 2018; Section 4, Number 8 of 2010 The Fines Act 2010.
[160] Section 18.1-2 Number 9 of 2018 Criminal Justice (Corruption Offences) Act 2018.

4.3 Storbritannien

4.3.1 U.K. Data Protection Act

U.K. Data Protection Act tillåter behandling av personuppgifter som avser begågna brott och fällande domar, om det är nödvändigt och har en skyddande funktion. Med skyddande funktion avses en funktion som är utformad för att skydda allmänheten mot oärlighet, felbehandling eller annat allvarligt oönskat beteende, obehörighet eller inkompetens, otillräcklig förvaltning av näringsverksamhet eller förening, eller fel i tjänster som tillhandahålls av en organisation eller en förening.[161] Utöver dessa bestämmelser måste vissa andra villkor också vara uppfyllda för att utgöra en laglig personuppgiftsbehandling, till exempel att behandlingen måste vara nödvändig med hänsyn till allmänintresse och lämpliga policydokument måste upprätthållas av den personuppgiftsansvariga.[162]

4.3.2 U.K. Bribery Act

U.K. Bribery Act ställer höga krav på verksamheter att förebygga och upptäcka korrupt beteende. Lagen har en extraterritoriell verkan för brittiska verksamheter utanför Storbritanniens territorium och andra företag med verksamhet i Storbritannien.[163] Verksamheten kan ådömas böter, vilken är obegränsad. I tillägg har personen som begår brottet ett personligt straffansvar, och kan dömas till fängelse upp till 10 år samt böter till ett obegränsat belopp.[164] Verksamheter kan undgå straffansvar genom att visa att relevanta riktlinjer med effektiv implementering, övervakning och uppföljning av dessa finns på plats i verksamheten. I tillägg är verksamheter skyldiga att se till att affärspartners har motsvarande rutiner för att förebygga korruption.[165]

[161] Section 10 (5), schedule 1, part 2, paragraph 11 U.K. Data Protection Act.
[162] Section 10 (5), schedule 1, part 2, paragraph 5-6 U.K. Data Protection Act.
[163] Borglund m.fl., s. 221.
[164] Section 11 U.K. Bribery Act.
[165] Cars, s. 178 f.

Lagen baseras på sex principer: Proportionerliga procedurer, ledningens engagemang, riskbedömning, tredjepartsbesiktning, kommunikation och utbildning samt övervakning och utvärdering.[166] Det är principerna om riskbedömning och framför allt tredjepartsbesiktning som är aktuella i detta sammanhang.

Den relevanta delen av regelverket går under namnet *kommersiella aktörers misslyckande att förhindra mutor* och innehåller tre sektioner: Kommersiella aktörers misslyckande att förhindra mutor, definition av associerad person och vägledning för kommersiella aktörer att förhindra mutor.[167] Den sist nämnda sektionen utgör ett lagstöd för *The U.K. Bribery Act Guidance* som är av största relevans för utredningen i det följande.

4.3.2.1 Riskbedömning

Principen beskrivs som en metod som antingen aktualiseras genom en affärsdrivande organisations verksamhetsmål eller genom en specifik metod som enbart syftar till att förebygga och upptäcka korruption. Riskbedömningen ska ta sikte på både interna och externa förhållanden, och genomföras regelbundet och grundligt samt dokumenteras. Riskbedömningen är uppbyggd med fem procedurer, varav *due diligence* är en av dessa.[168] Den externa riskbedömningen ska utgå från fem faktorer, nämligen geografiska risker, branschrisker, transaktionsrisker, affärsrisker och affärsrelationsrisker.[169]

Geografiska risker

Den geografiska lokaliseringen kan innebära högre risk för korruption. I bedömningen ska hänsyn tas till landets eller områdets avsaknad eller implementering av antikorruptionsrelaterad reglering och avsaknad av reglering i förmån för transparanta upphandlingar och investeringar inom statsledningen, media, lokala näringslivet och det civila samhället.[170]

[166] The U.K. Bribery Act Guidance, s. 21-31.
[167] Section 7-9 U.K. Bribery Act.
[168] The U.K. Bribery Act Guidance, s. 25.
[169] Ibid, s. 26.
[170] Ibid.

Bransch- och transaktionsrisker

Vissa sektorer kan innebära högre risk för korruption. Här anges utvinningsindustrin och storskaliga infrastrukturinvesteringar som högrisksektorer. Vissa transaktioner kan innebära högre risk för korruption. Här anges välgörande eller politiska transaktioner, licenser eller tillstånd och offentlig upphandling som högrisktransaktioner.[171]

Affärs- och relationsrisker

Affärsmöjligheter anges vara en riskfaktor som kan uppstå i högkostnadsprojekt som involverar många aktörer, när projektkostnader inte följer marknadspriset eller när projektet saknar tydliga och legitima intressen. Vissa affärsrelationer kan innebära högre risk för korruption. Här anges finansiella mellanhänder i transaktioner med utländska statstjänstemän, konsortium och *joint ventures* samt transaktioner med politiskt exponerade personer där affärsrelationen involverar eller är kopplad till en inflytelserik statstjänsteman.[172]

Den interna riskbedömningen tar även den sikte på fem faktorer, nämligen bristande personalutbildning, bonuskultur som uppmanar överdrivet risktagande, bristande policys om och procedurer för representation och politiska eller välgörande bidrag, bristande finansiell kontroll och slutligen avsaknad av avståndstagande från ledningen avseende korrupt beteende.[173]

4.3.2.2 Tredjepartsbesiktning

En affärsdrivande organisation kan hållas ansvarig för det fall en associerad person till organisationen begår mutbrott i syfte att erhålla eller behålla en affärsrelation eller affärsmöjlighet å organisationens vägnar. Med *associerad person* avses en fysisk eller juridisk person som utför tjänster till eller å organisationens vägnar, vilken även omfattar anställda.[174] Definitionen innebär att principen får ett brett tillämpningsområde eftersom många olika typer av affärsrelationer omfattas, vilket kräver en anpassningsbar metod för

[171] The U.K. Bribery Act Guidance, s. 26.
[172] Ibid.
[173] Ibid.
[174] Section 8 U.K. Bribery Act; The U.K. Bribery Act Guidance, s. 16, p. 37.

kontroll utifrån den i fallet relevanta affärsrelationen. Principen innebär att varje affärsdrivande organisation med ett proportionerligt och riskbaserat tillvägagångssätt ska kontrollera associerade personer, i syfte att minska de identifierade korruptionsriskerna. Kontrollen kan genomföras av interna eller externa konsulter och proportionaliteten ska bedömas i förhållande till den identifierade risken.[175]

Principen syftar också till att uppmuntra kommersiella organisationer att införa kontrollmekanismen i förebyggande syfte för att förhindra affärspartnern att begå mutbrott å organisationens vägnar.[176] Här föreslås att en grundlig kontroll genomförs i samband med rekryteringsförfarande, särskilt vad gäller högre tjänster eller inom jurisdiktioner där det är svårare att avsluta en redan inledd affärsrelation. Genomförandet av tredjepartsbesiktning anges också vara särskilt angeläget vid tillfälle av företagsförvärv och företagsöverlåtelser.[177]

I en bilaga till principen ges exempel på åtgärder som organisationer kan vidta, tillsammans eller var för sig, innebärande frågeformulär, uppdragsbeskrivning, bakgrundskontroller, inhämtande av myndighetsinformation, kontakta referenser, kontrollera anti-korruptionspolicys, kontrollera expertis samt regelbundna kontroller.[178] Frågeformuläret ska efterfråga ägarskapsdetaljer, CV, referenser för samtliga potentiella involverade, detaljer om chefspositioner, existerande avtal och samarbetspartners och andra relevanta judiciella och regulatoriska omständigheter. Tjänsten eller uppdraget ska konkret och detaljerat beskriva vad tjänsten eller uppdraget innebär, inklusive kostnader, provision, arvode och förväntad lön. Den potentiella affärspartnern ska också undersökas vad gäller personerna i ledande befattningar, och för att verifiera framkommen information genom frågeformuläret ska myndighetsupplysningar samt referenser inhämtas. Detta kan kräva personliga möten. Verksamhetsutövaren kan också behöva efterfråga syn eller bevis på den potentiella partnerns

[175] The U.K. Bribery Act Guidance, s. 27.
[176] Ibid, s. 27.
[177] Ibid, s. 27 f.
[178] Ibid, appendix A, s. 38.

påstådda antikorruptionspolicys, inklusive åtgärdsprogram och rutiner för dokumentation. Det är i tillägg nödvändigt att verksamhetsutövaren värderar frågor om partnern verkligen behövs, om denne besitter den efterfrågade expertisen, om det finns några kopplingar till statstjänstemän samt om ersättningen för uppdraget eller tjänsten är rimlig och marknadsmässig. Om affärsrelationen efter dessa kontroller inleds så ska *due diligence* genomföras kontinuerligt under relationens gång.[179]

4.4 Frankrike

4.4.1 Lagen om datainformation

Nationella kommissionen för informatik och friheter[180] utarbetar och publicerar i samråd med offentliga och privata aktörer standardbestämmelser för att säkerställa säkerheten hos personuppgifter och för att reglera behandlingen av hälsodata. Från detta får det upprättas undantag för personuppgiftsbehandlingar, utöver de personuppgiftsbehandlingar som genomförs av offentliga myndigheter, som föreskriver ytterligare tekniska och organisatoriska åtgärder för behandling av biometriska, genetiska och medicinska uppgifter och ytterligare garantier för behandling av överträdelsesdata i enlighet med art. 10 i GDPR.[181] Fysiska personens rättigheter kan begränsas i enlighet med lagen om datainformation så länge en sådan begränsning utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle. Till detta ska beaktas de grundläggande rättigheterna och legitima intressen för den aktuella individen i syfte att till exempel undvika skada, förebygga, upptäcka eller utreda brott eller verkställa straffrättsliga påföljder. Sådana begränsningar kan till exempel innebära begränsning av kommunikation och underrättelse om användning av individens uppgifter.[182]

[179] The U.K. Bribery Act Guidance, appendix A, s. 38.
[180] *La Commission nationale de l'informatique et des libertés.*
[181] Art. 11.I.2.b lagen om datainformation.
[182] Art. 70-21 lagen om datainformation.

4.4.2 Sapin II

Den franska antikorruptionslagstiftningen *Sapin II* omfattar alla verksamheter inom den privata och offentliga sektorn som är etablerade i Frankrike. Lagen är extraterritoriell på så sätt att nämnda verksamheter omfattas oavsett om affärshandlingarna vidtas utomlands, såtillvida det aktuella landets lag inte är mer rigorös avseende förebyggande och bekämpande av korruption.[183] Art. 17 i *Sapin II* kräver att styrelsemedlemmar, verkställande direktörer och chefer för verksamheter med minst femhundra anställda eller som tillhör en koncern vars moderbolag har sitt huvudkontor i Frankrike och vars arbetskraft omfattar minst femhundra anställda, och vars omsättning eller konsoliderade omsättning är större än 100 miljoner euro vidtar åtgärder som syftar till att förebygga och upptäcka korruption, i Frankrike eller utomlands.[184]

Vid åsidosättande av de skyldigheter som anges i art. 17 föreligger straffansvar för verksamheten som juridisk person. Tillsyn och övervakning av efterlevnad sker av *Agence Française Anticorruption* (AFA). Kontroller genomförs genom att verksamheter inger rapporter till den myndighet som begärt kontrollen och till verksamhetens företrädare. Rapporten ska innehålla byråns iakttagelser om kvaliteten på det förebyggande och bekämpande systemet mot korruption samt om nödvändigt ge rekommendationer för förbättring av det interna kontrollsystemet.[185] Om brott uppdagas kan den ansvariga beslutsfattaren på byrån utfärda varningar till verksamhetens företrädare. Verksamheten och dess företrädare kan också föreläggas att anpassa interna förfarandena för att förebygga och upptäcka korruption, samt ålägga ekonomiska påföljder för fysiska och juridiska personer.[186] Den ekonomiska påföljden uppgår till 200 000 euro för fysiska personer och en miljon euro för juridiska personer. Beloppet ska stå i proportion till huruvida de konstaterade överträdelserna är allvarliga eller ej och till den fysiska eller juridiska personens ekonomiska situation.[187]

[183] AFA Guidelines, s. 3.
[184] Art. 17 Sapin II.
[185] Art. 17.III Sapin II.
[186] Art. 17. IV Sapin II.
[187] Art. 17. V Sapin II.

Som ett tillägg till *Sapin II* finns riktlinjer för att hjälpa verksamheter att upprätta och strukturera complianceprogram som en del av bedömning och hantering av risker vad gäller verksamhetens ekonomi och anseende. Riktlinjerna är tillämpliga för alla typer av verksamheter oavsett storlek eller verksamhetsform, men är *per se* inte juridiskt bindande.[188] Åtgärderna som ska vidtas i verksamheten är en mängd olika. En uppförandekod ska upprättas som definierar och illustrerar de olika typerna av beteende som är förbjudna, som sannolikt är att karakterisera som korruptionshandlingar. Uppförandekoden ska vara införlivad i verksamhetens interna bestämmelser och blir i samband med detta föremål för franska arbetsrättsregler.[189] Det ska finnas ett internt varningssystem som möjliggör insamling av rapporter från anställda avseende förekomsten av beteenden eller situationer som strider mot verksamhetens uppförandekod.[190] Till detta ska det finnas disciplinära åtgärder för den som bryter mot uppförandekoden.[191]

Identifiering och analysering av risker för korruption som finns vid verksamhetens utövande utomlands ska kartläggas och regelbundet dokumenteras, särskilt i förhållande till verksamhetsområdet och det geografiskt aktuella området.[192] Det ställs krav på att rutiner för interna eller externa bokföringskontroller ska upprättas, avsedda för att säkerställa att räkenskapsböcker, register och konton inte används för att dölja korruption. Dessa kontroller kan utföras antingen av en intern redovisnings- eller finansiell kontrolltjänst eller genom en extern revisor.[193] Chefer och personal som är mest utsatta för riskerna med korruption ska tillförses med utbildning inom området, och det ska finnas ett system för intern kontroll och utvärdering av verksamhetens genomförda åtgärder.[194] Det ska också finnas ett upprättat system för att undersöka kunder, leverantörer och mellanhänders situationer i samband med riskanalysen, med andra ord tredjepartsbesiktning.[195]

[188] AFA Guidelines, s. 4.
[189] Art. 17. 1° Sapin II.
[190] Art. 17. 2 ° Sapin II.
[191] Art. 17. 7 ° Sapin II.
[192] Art. 17. 3 ° Sapin II.
[193] Art. 17. 5 ° Sapin II.
[194] Art. 17. 6 och 8° Sapin II.
[195] Art. 17. 4° Sapin II.

4.4.3 AFA Guidelines

AFA Guidelines är ett verktyg för efterlevnaden av *Sapin II*. *AFA Guidelines* belyser vikten av att organisationer utför *due diligence* med sikte på affärspartners integritet för att undvika involvering i korrupta affärshandlingar. En inblandning i korrupta affärer utgör juridiska, kommersiella och ekonomiska risker samt sätter verksamhetens anseende på spel. Analysen som en *due diligence* innebär ska innehålla en kartläggning av information och dokument om affärspartnern, som läggs till grund för en riskbedömning avseende korrupt beteende och således även ett beslut huruvida affärsrelationen ska inledas alternativt fortskrida eller ej.[196] En efterlevnad av de franska riktlinjerna kan hjälpa verksamheten att uppfylla lagkraven.[197]

4.4.3.1 Tillvägagångssätt

Vid en inledd affärsrelation rekommenderar *AFA Guidelines* att en *due diligence* genomförs frekvent i den utsträckning som lämpar sig för branschen i fråga i förhållande till dess korruptionsrisker, och när det på grund av nya omständigheter är relevant att uppdatera riskbedömningen, till exempel vid företagsförvärv, ändringar av bolagsordning och ändringar i bolagsledningen.[198] Syftet med riskbedömningen anges vara dels en markör för affärsrelationens status, dels en effektivitetsökning för vidtagandet av åtgärder för att förebygga och upptäcka korruption.[199] Vidare rekommenderas ett upprättande av en databas innehållande tredje parter eller ett informationssystem för att underlätta behandlingen av uppgifterna. Detta ska då genomföras i enlighet med de principer och processer som fastställs i Lag om datainformation.[200]

[196] AFA Guidelines, s. 19.
[197] Ibid, s. 4.
[198] Ibid, s. 19 p. 1.
[199] Ibid, s. 19 p. 2.
[200] AFA Guidelines, s. 20 p. 3 och not 6.

Enligt *AFA Guidelines* ska riskbedömningen involvera tre nivåer i organisationen, nämligen verksamhetschefer, *compliance officer*[201] och bolagsledningen. Verksamhetschefer ska genomföra *due diligence* och bär ansvaret för densamma. Analysen ska sedan presenteras, vilken kan ligga till grund för en slutlig bedömning i lågriskfall. *Compliance officer* ska bistå med expertis, rådgivning och stöd till verksamhetschefer i högriskfall. Bolagsledningen ska göra de slutliga besluten i högriskfallen som har identifierats av verksamhetschefer.

Samarbete mellan de tre nivåerna rekommenderas för att undvika operativa fel, intressekonflikter och bedrägeri. Om det anses nödvändigt får tredjepartsbesiktning utföras av en utomstående aktör, särskilt i de fall då verksamheten inte avser att behålla den information som införskaffas under processen eller då parten som ska kontrolleras befinner sig eller utövar sin verksamhet i ett land där kontrollerande verksamheten inte är representerad.[202] Vilken typ av information som ska anses vara av relevans för undersökningen ska bedömas utifrån kartläggningen av risker, verksamhetens struktur och intressen. Det kan till exempel vara insamlande av offentligt tillgänglig eller allmän information som domar och tidningsartiklar, kontrollera huruvida tredje parten eller dess ägare är föremål för sanktioner, kontrollera huruvida tredje partens nyttjanderättsägare eller verksamhetsledning inkluderar en politiskt exponerad person, samla information från kommersiella databaser och samla information direkt från tredje parten i form av intervjuer, frågeformulär, revision och interna auktorisationer eller certifikat.[203]

4.4.3.2 Bedömningsgrunder

Verksamheter ska försäkra sig om att användningen av en tredje part är berättigad och möter ett reellt behov. Det bör framgå varför en viss part har utsetts för genomförandet av uppdraget, istället för en konkurrerande tredje part. Att en klient rekommenderar eller kräver en specifik tredje part är en

[201] Sakkunnig inom området för aktuell regelefterlevnad.
[202] AFA Guidelines, s. 20 p. 4.
[203] Ibid, s. 20 f.

varningssignal för oegentligheter. *Due diligence* ska genomföras så att innehållet är i enlighet med regelverk som dataskydd, penningtvätt och konkurrens. *AFA Guidelines* rekommenderar att innehållet består av identitet, ägarskap, geografiska risker, branschsektor, kompetens, integritet och anseende, *compliance*, samarbeten, affärsrelationens karaktär och syfte, aktörer, koppling till statstjänstemän eller politisk exponerade personer, finansiella överväganden, ekonomisk kompensation och betalningsprocesser.[204]

Identitet och ägarskap

Verksamheter bör försäkra sig om de viktigaste delarna av tredje partens identitet, så som namn, företagsnamn, juridisk struktur, datum för bolagsregistrering, antal anställda, omsättning, bokfört kapital, affärssektor, kvalifikationer och lokalisering. Verksamheter bör även försäkra sig om aktieägares och nyttjanderättsägares namn, i den mån de aktuella individerna eller entiteterna direkt eller indirekt äger minst tjugofem procent av andelarna eller rösträtterna, eller i annat fall den individ eller entitet som leder förpliktande kollektiva investeringar.[205]

Geografiska risker

Som en del av kartläggningen av riskerna bör riskerna graderas i förhållande till det geografiska området, baserat på verksamheternas erfarenheter. Bedömningen bör även ta hänsyn till offentligt publicerade listor över ländernas föremål för sanktioner ålagt av ekonomiska och finansiella departement, OECD:s övervakningsrapporter över implementering av Konventionen för bekämpandet av mutor för utländska statstjänstemän i internationella affärer och CPI som årligen publiceras av *Transparency International*. Under genomförandet av *due diligence* ska landet för partens vistelseort undersökas, samt de länder där tredje parten och dess verksamhet är registrerade. Exempel på länder som utgör risker är de som inte utgör en samarbetsjurisdiktion eller ett land utan jämförbart regelverk.[206]

[204] AFA Guidelines, s. 21.
[205] Ibid.
[206] Ibid.

Branschsektor

Verksamheter bör etablera en procedur för att rangordna korruptionsrisker i förhållande till sektorer. Dessa bör uppdateras regelbundet och med hänsyn till landets korruptionsrisker och verksamhetens egna erfarenheter. I tillägg bör hänsyn tas till *Transparency International Bribes Payer Index Report*. Under genomförandet av *due diligence* bedöms sektorsriskerna utifrån den risknivån som är aktuell i den branschen där tredje parten tjänar sin inkomst.[207]

Kompetens, integritet och anseende

Verksamheter bör säkerställa att tredje parten besitter de erfarenheterna, kvalifikationerna och kunskaperna som krävs för att utföra den aktuella tjänsten. För detta syftet får verksamheten be tredje parten om relevanta referenser, beroende på den data som redan har insamlats avseende tredje partens verksamhet. Bristande kvalifikationer och expertis kan utgöra en försvårande faktor vid bedömningen, likaså bör det kontrolleras om den ekonomiska ersättningen motsvarar nivån på expertisen och tjänsten som utförs. Verksamheter bör försäkra sig om tredje parten, dess aktieägare, nyttjanderättsinnehavare och ledning har varit föremål för negativ information, anklagelser, åtal eller dömts för brott och speciellt brott relaterade till korruption. Tredje partens risknivå bör bli justerad i enlighet med vad som framkommer vid en sådan undersökning.[208]

Compliance och samarbete

Verksamheter bör undersöka huruvida tredje parten har utvecklat en antikorruptionspolicy eller ej. En part som inte nämner eller dokumenterar sådan implementering kan utgöra en riskhöjande faktor. Tredje partens beteende bör beaktas vid riskbedömningen. En parts förvägran att tillförse efterfrågad information eller dokument kan utgöra en riskhöjande faktor. [209]

[207] AFA Guidelines, s. 21 f.
[208] Ibid, s. 22.
[209] Ibid.

Affärsrelationens karaktär och syfte

Verksamheter bör definiera och specificera de krav för utförande som kontraktet ställer, eftersom riskbedömningen varierar beroende på affärsrelationens karaktär och syfte. Vissa typer av affärsrelationer innebär höga korruptionsrisknivåer, till exempel den tredje part som ska hjälpa verksamheten att vinna upphandlingar. Å ena sidan kan verksamheten uppmuntra tredje part att vidta oegentliga affärsmetoder för att kringgå den egna anti-korruptionspolicyn. Å andra sidan kan tredje part engagera sig i sådana aktiviteter på eget initiativ utan att informera verksamheten.[210]

Ytterligare aktörer, offentligt anställda och politiskt exponerade personer

Verksamheter kan ingå i affärsuppgörelser som innebär flera aktörer, utan att direkt vara i samröre med dessa. I sådana fall bör verksamheter försäkra sig om att tredje parten för sin egen del utför tredjepartsbesiktning avseende dessa aktörer. Affärer mellan den privata och publika sektorn utgör en hög korruptionsrisk. Verksamheter bör identifiera affärerna som tredje part kan vara involverad i med den offentliga sektorn och notera statstjänstemännens namn och huruvida de är politiskt exponerade eller ej. En sådan exponering kan innebära en förhöjd korruptionsrisk. [211]

Finansiella överväganden och ekonomisk kompensation

En långvarig eller högt finansiellt värderad affärsrelation kan innebära en förhöjd riskfaktor. Vilken valuta som används bör också noteras, men hänsyn till den extraterritoriella verkställigheten av vissa länders regelverk gällande antikorruption. Ersättning för leverantörer, agenter och andra aktörer bör vara konsekvent i förhållande till den vara eller tjänst som förmedlas samt mängd sålda av tredje parten och i enlighet med marknadspriser. Om inkonsekvens uppdagas bör det pågående *due diligence*-förfarandet avbrytas till dess att en rimlig förklaring finns. Provision för tilldelat kontrakt är en högriskfaktor i bedömningen av tredje parten. [212]

[210] AFA Guidelines, s. 22.
[211] Ibid, s. 23.
[212] Ibid.

Betalningsprocesser

Tredje partens placering av banktillgångar kan vara en försvårande faktor i riskbedömningen, till exempel om banken befinner sig i en icke samarbetsvillig jurisdiktion. Verksamheter bör försäkra sig om att de efterfrågade betalningsprocesserna är förenliga med rådande praxis. Kontanta och gränsöverskridande betalningar, betalningar till utomstående aktör annan än aktuell tredje part och betalningar för ospecificerade fakturor är att anse som riskhöjande faktorer.[213]

4.4.3.3 Bedömning

Bedömningen avseende tredje partens risknivå bör utföras i två steg. För det första ska en bedömning göras baserat på objektiva och kvantifierbara faktorer som sanktioner, affärssektor, registreringsdatum etc. För det andra ska de kvalitativa faktorerna analyseras, som till exempel riskförhöjande faktorer och samarbete. Risknivån enligt bedömningen i första steget får revideras i uppgående eller nedåtgående led med hänsyn till det kvalitativa kriteriet. I slutskedet ska riskbedömningen avseende tredje parten vara klassificerad i risknivåerna låg, medel och hög.[214] Bedömningen ska leda till ett beslut om godkänd, avslutad eller icke inledd affärsrelation. Ett beslut kan också skjutas upp vid behov av ytterligare undersökningar.[215]

Bedömningen ska göras av en person utsedd i enlighet med affärsrelationens aktuella läge, tredje partens kategori och dennes risknivå. En *due diligence* som inte påvisar några riskfaktorer innebär inte en riskfri affärsrelation till tredje parten, men det är inte heller alltid nödvändigt att avsluta en affärsrelation då risker har identifierats. Det gäller att vidta rätt åtgärder för att förebygga och upptäcka korruption.[216]

4.4.3.4 Förebyggande åtgärder

Åtgärder för att förebygga och upptäcka korruption bör anpassas efter varje organisationsmiljö, vilket innebär att det är upp till varje verksamhet att

[213] AFA Guidelines, s. 23.
[214] Ibid, p. 6.
[215] Ibid, p. 7.
[216] Ibid.

definiera åtgärderna på ett sätt som är förenligt med verksamhetsmodellen. Det kan till exempel göras genom att informera och utbilda tredje parten om verksamhetens antikorruptionspolicy, kräva att tredje parten följer verksamhetens policy, inkorporera en antikorruptionsklausul i avtal och kräva att tredje part verifierar underleverantörers integritet.[217]

Avtal

Avtal med tredje parter bör övervakas i syfte att förebygga och upptäcka korruption. Kontrakt bör inkludera specifika villkor för avtalets genomförande samt kompensationens storlek och procedur. För att uppnå detta måste verksamheten ha omfattande översikt över tredje partens in- och utbetalningar, så att verksamheten kan försäkra sig om att kompensationer och betalningar har genomförts i enlighet med avtalsvillkoren. Verksamhetens finansiella avdelning bör meddela complianceansvarig när ovanliga betalningar efterfrågas, till exempel kontanta utbetalningar eller ändring av bankkonto till en bank i en icke samarbetsvillig jurisdiktion.[218] *Due diligence* bör genomföras regelbundet, med tidsintervaller beroende på tredje partens risknivå. Sådana kontroller bör framgå vid avtalets ingående. Särskilda situationer ger anledning att omedelbart genomföra en ny kontroll, till exempel vid anledning av tredje parts inblandning i företagsförvärv.[219]

Trelinjeförsvar

Granskning av genomförd *due diligence* omfattar tre så kallade försvarslinjer. Första granskningen genomförs av den i första hand ansvariga för hela undersökningens praktiska genomförande. En andra granskning genomförs av complianceansvarig i syfte att verifiera en ordentligt genomförd granskning på första nivån. Tredje kontrollen genomförs av den interna redovisningsavdelningen för att försäkra sig om att genomförd *due diligence* är förenlig med verksamhetens krav, fullt implementerad och uppdaterad.[220] *AFA Guidelines* rekommenderar även att det ska upprättas ett system för att övervaka *due diligence*-processerna. Det kan till exempel innebära mätning av slutförda *due diligence*-processer, hur ofta regelbundna kontroller görs,

[217] AFA Guidelines, s. 24 p. 7.1.
[218] Ibid, p. 7.2.
[219] Ibid, p. 7.3.
[220] Ibid, p. 8.

statistik över upptäckter i första- och andrastegsgranskningarna och en åtgärdsplan för de situationer då det i första- och andrastegsgranskningen uppdagas en otillräcklig eller oavslutad undersökning.[221] Samtliga genomförda undersökningsprocesser bör sparas i fem år efter avslutad affärsrelation.[222]

4.5 USA

4.5.1 FCPA

USA inrättade under 1970-talet ett av världens mest framstående regelverk mot korruption, *Foreign Corrupt Practices Act* (FCPA).[223] Lagen omfattar inhemska eller utländska personer och enheter som är noterade på amerikanska börsen, har sin huvudsakligen verksamhet i USA, finansiella institut som är skyldiga att upprätta rapporter eller ansöka om licenser enligt amerikansk lag samt utländska personer eller företag vars affärer sker på amerikanskt territorium. I tillägg kan andra företag som är associerade med nämnda kategorier omfattas.[224] Samtliga nämnda kategorier förbjuds enligt *FCPA* att genom korrupta betalningar till utländska statstjänstemän behålla eller förvärva affärsförbindelser.[225] Straffen som kan aktualiseras är både straffrättsliga och civilrättsliga böter, vilka ligger mellan 10 000 till två miljoner amerikanska dollar för juridiska personer och mellan 10 000 till 100 000 amerikanska dollar samt fängelse upp till fem år för fysiska personer. Vad gäller inlämnande av falska eller vilseledande uppgifter av organisationer som är skyldiga att rapportera eller ansöka om licens enligt amerikansk lag aktualiseras böter upp till 25 miljoner amerikanska dollar för juridiska personer och fem miljoner amerikanska dollar samt fängelse upp till 20 år för fysiska personer.[226]

[221] AFA Guidelines, s. 24 p. 9.
[222] Ibid, p. 10.
[223] Cars, s. 177.
[224] FCPA Guide, s. 10.
[225] Ibid, s. 2.
[226] Title 15 Commerce and Trade, Chapter 2B Securities Exchanges § 72dd-2 Prohibited foreign trade practices by domestic concerns (g), § 78dd-3 Prohibited foreign trade practices by persons other than issuers or domestic concerns (e) och § 78ff, FCPA.

FCPA fastställer att justitieministern i samråd med andra myndigheter ska upprätta riktlinjer för de krav som ställs av regelverket.[227] *FCPA Guide* är inte ett juridiskt bindande dokument, men uppställer en rad olika verktyg och faktorer för organisationer att ta hänsyn till vad gäller regelefterlevnaden av *FCPA*.[228] Vägledningen utgår i mångt och mycket från hur dessa myndigheter arbetar och vilka faktorer som är av relevans i det utredande arbetet.[229]

4.5.2 Tredjepartsbesiktning

Kravet på tredjepartsbesiktning är integrerat i olika bedömningspunkter i stor utsträckning. Kapitel fem i *FCPA Guide* erbjuder en komprimerad informativ lista över vad ett complianceprogram bör innehålla, grundat på myndigheternas bedömningspunkter vid eventuella åtal. Complianceprogram utgör en stor del av skuldfrågan och således även vilken form av påföljd som ska aktualiseras. Ett välstrukturerat, implementerat och ändamålsenligt complianceprogram kan medföra att myndigheter underlåter att väcka åtal, på så sätt att organisationen har gjort allt i sin makt för att i sin verksamhet förhindra, upptäcka, avhjälpa och rapportera oegentligheter. Om ett complianceprogram saknas eller ett bristfälligt sådant uppvisas står organisationen och personer i ledande ställning inför kraftiga sanktioner.[230] I en utvärdering publicerad av amerikanska justitiedepartementet presenteras en detaljerad lista över faktorer för åklagare att ta hänsyn till vid bedömningen av complianceprogrammets effektivitet vid tidpunkten för den korrupta händelsen, men även vid tidpunkten för åtalsbeslutet. Utvärderingen av complianceprogrammets påverkar sedan bedömningen var gäller åtal eller lämplig tvistlösning, bötesstraff och huruvida organisationen ska åläggas så kallade complianceåtgärder, till exempel övervakning eller rapporteringsskyldighet. Rent praktiskt innebär det att en organisation kan tvingas att på egen hand upprätta eller genom en av myndigheten utsedd person infinna sig i ett complianceprogram. Organisationen kan också

[227] Title 15 Commerce and Trade, Chapter 2B Securities Exchanges § 78dd-1 [Section 30A of the Securities & Exchange Act of 1934] (d) och § 72dd-2 Prohibited foreign trade practices by domestic concerns (e), FCPA.
[228] FCPA Guide, s. 2.
[229] Ibid, s. 57.
[230] Ibid, s. 56 ff.

drabbas av uteslutning från handel med den offentliga sektorn och indragna eller inskränkta export- och importrättigheter.[231] Bedömningsstrukturen följer tre huvudfrågor, nämligen huruvida programmet är väl utformat, effektivt implementerat och praktiskt genomförbart. [232] Frågan om *due diligence*, tillsammans med riskbedömning, policys, utbildning, rapporterings- och utredningskanaler och företagsförvärv, faller därmed under den förstnämnda bedömningsfrågan.

4.5.2.1 Riskbedömning

Riskbedömningen ska, med en förståelse för organisationens affärer från ett kommersiellt perspektiv, ta hänsyn till faktorer som affärens lokalisering, industrisektor, konkurrens på marknaden, det regulatoriska landskapet, potentiella klienter och affärspartners, transaktioner med utländska myndigheter, användning av tredje parter och utgifter för bland annat gåvor, välgörenhet och resor.[233]

4.5.2.2 Tredjepartshantering

Som en del av riskbedömningen ska organisationen utföra *due diligence* inför transaktioner till tredje parter, till exempel agenter, konsulter och distributörer. Dessa yrkeskategorier används ofta för att dölja oegentligheter. Riskbedömningen ska innebära att organisationen skapar sig en förståelse för tredje partens kvalifikationer och associationer och skapar sig kännedom om tredje partens anseende och affärsrelationer, samt finner det affärsmässigt motiverat att använda sig av denne. Avtalet ska specifikt reglera tjänsten som ska utföras och organisationen ska följa upp att det avtalade utförs samt ersättningen är marknadsmässig för det utförda arbetet i den aktuella regionen eller branschen. Organisationen ska genomföra kontinuerlig övervakning över sina affärsrelationer genom till exempel tredjepartsbesiktning, personalträning, revision och årliga compliancecertifikat för tredje parten.[234]

[231] FCPA Guide, s. 69 ff.
[232] Evaluation of Corporate Compliance Programs, s. 1 f.
[233] Ibid, s. 6 ff.
[234] Ibid.

Sammanfattningsvis är ett företags genomförande av tredjepartsbesiktning är en faktor som åklagare ska bedöma för att avgöra om ett complianceprogram är tillräckligt för att upptäcka branschspecifika typer av oegentligheter.[235]

Riskbaserad och integrerad process

Hänsyn ska tas till företagets hantering av tredje part och hur hanteringen har korresponderat med affärens natur och tidigare identifierade risker. Det är även av relevans hur denna process har integrerats i upphandling och inköpsprocesser.[236]

Passande kontroller

I bedömningen ska hänsyn tas till hur företaget försäkrar sig om att det är affärsmässigt motiverat att använda sig av tredje parten. Om det skulle visa sig att tredje parten var inblandad i oegentligheter ska företaget kunna redovisa det affärsmässiga motivet för användningen av partnern. Av relevans är också vilka mekanismer som företaget använder för att försäkra sig att avtalet är tillräckligt specificerat vad gäller tjänsten, servicen eller uppdraget, ersättning, tillförlitliga betalningsmetoder, att tjänsten utförs avtalsenligt och att ersättningen är proportionerlig i förhållande till tjänsten.[237]

Hantering av affärsrelationer

Företagets tillvägagångssätt för att överväga och analysera ersättning och incitamentsstrukturer för tredje parter i förhållande till compliancerisker är relevant för bedömningen. Detta kontrolleras bland annat genom hur företaget övervakar sina tredje parter, om företaget har revisionsrättigheter att analysera tredje partens bok- och kontoföring, och om företaget i så fall har utnyttjat den möjligheten. Hänsyn ska också tas till hur företaget utbildar sina tredje parter om hantering av compliancerisker, och hur företaget ger incitament till tredje parter att uppföra sig etiskt och i enlighet med företagets *compliance*.[238]

[235] Evaluation of Corporate Compliance Programs, s. 7.
[236] Ibid.
[237] Ibid.
[238] Ibid, s. 7 f.

Faktiska åtgärder och konsekvenser

Hur företaget bemöter och hanterar de röda flaggor som eventuellt identifieras genom tredjepartsbesiktning är en del av bedömningen. Detta innebär även frågor om företaget håller koll på de tredje parter som inte har klarat företagets undersökning eller blivit avstängda, och hur företaget försäkrar sig att dessa tredje parter inte återanlitas. Om en tredje part visar sig involverad i oegentligheter, ska företaget kunna visa hur röda flaggor identifierades under genomförandet av *due diligence* eller efter anlitandet. Det är också av relevans om en liknande tredje part tidigare har blivit avstängd eller fått sina räkenskaper kontrollerade på grund av compliancearbetet på företaget.[239]

4.5.2.3 Företagsförvärv

Genomförande av tredjepartsbesiktningen inför ett företagsförvärv underlättar riskbedömningen för köparen vad gäller att identifiera oegentligheter och på förhand kunna uppskatta kostnader med anledning av eventuella oegentligheter. En bristfällig *due diligence* kan innebära att eventuella oegentligenheter hos det förvärvade företaget fortskrider och åsamkar köparen stora skador, både ekonomiska och anseendemässiga. Bedömningen tar sikte på om oegentligheter eller risker identifierades under genomförandet av *due diligence* och i så fall vem som övervakade riskanalysen gällande den förvärvade enheten och hur övervakningen genomfördes. Det är också av relevans hur compliancefunktionen har blivit integrerad i förvärvet och medföljande processer, samt hur företagets system för att följa upp och förhindra oegentligheter eller risker ser ut.

[239] Evaluation of Corporate Compliance Programs, s. 8.

5 Analys

5.1 Regelkonflikt

Som konstaterats i avsnitt 3 omfattar GDPR all personuppgiftsbehandling som sker i yrkes- och näringsverksamhet avseende fysiska personer och omfattar verksamheter etablerade inom EU och under vissa omständigheter även verksamheter etablerade utanför EU. Myndigheter har genom GDPR större möjligheter att behandla personuppgifter, medan privata aktörers möjligheter att behandla personuppgifter i många fall styrs av nationell reglering. För att privata aktörer ska få undantas från vissa skyldigheter enligt GDPR ställs höga krav på att undantaget är en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle för att skydda allmänna intressen. Vad som utgör allmänna intressen är inte helt självklart, och med bristande vägledning från EU kan det möjligen resultera till att begreppets innebörd varierar från medlemsstat till medlemsstat, vilket försvårar förståelsen för begreppet.

En del av tredjepartsbesiktning utförs genom att kontrollera brottsuppgifter och politisk involvering avseende individer inblandade i affärsavtal. Att behandla sådana uppgifter möter direkta hinder på grund av GDPR, så länge det inte finns nationell eller unionsrättslig reglering som tillåter personuppgiftsbehandlingen i ett korruptionsförbyggande syfte. Skälen till GDPR ger flertalet gånger stöd för medlemsstater att införa nationella undantagsregler för personuppgiftsbehandling för att förebygga och upptäcka korruption. Det går att ställa sig frågan varför området inte reglerades som ett undantag direkt i GDPR. Det borde nämligen inte framstått som helt osannolikt att en potentiell regelkonflikt med diverse olika nationella lösningar skulle kunna skapa en obalans mellan medlemsstater och påverka den inre marknaden. Väl vedertagna internationella standarder med syftet att förebygga och upptäcka korruption förlorar sin betydelse för verksamheter inom unionsgemenskapen, vilket påverkar affärsrelationer på en global nivå, till exempel då affärsavtal omfattas av den amerikanska lagstiftningen *FCPA*. Verksamheter i de medlemsstater som inte har behandlat frågan om undantag från GDPR för tredjepartsbesiktning hamnar i ett sämre affärsmässigt läge

jämfört med verksamheter i tredje land eller medlemsstater som reglerat frågan.

5.2 Nationella lösningar

Storbritannien, Irland och Frankrike var snabba på att införa undantagsregler som tillåter personuppgiftsbehandling av brottsuppgifter med syftet att förebygga och upptäcka korruption. Storbritannien och Frankrike har utformat antikorruptionsregleringar som utgör starka rättsliga förpliktelser i GDPR:s mening. *U.K. Bribery Act* säkerställer till exempel existensen av den vägledning näringsidkare kan följa för att undgå straffansvar. Det finns goda argument för att förebyggande och tidigt upptäckande av korruption anses vara av väsentligt allmänt intresse i Storbritannien. *U.K. Bibery Act* antagen 2010 förbjuder bestickning av utländska tjänstemän och ålägger företag straffrättsligt ansvar för korrupta handlingar av associerade personer. Vägledningen *The U.K. Bribery Act Guidance* utgiven samma år förtydligar företagens skyldighet att förhindra mutor av associerade personer enligt *U.K. Bribery Act*, genom till exempel riskbaserad *due diligence* och adekvata förfaranden för att förhindra mutor av associerade personer. Det finns alltså god anledning att anta att de brittiska myndigheterna avsåg att fastställa upptäckt och förebyggande av korruption som ett väsentligt allmänt intresse genom *U.K. Bribery Act* och den tillhörande vägledningen, se avsnitt 4.3.

Sapin II utgör en rättslig förpliktelse, men endast i viss begränsad utsträckning. *AFA Guidelines* är genom *Sapin II* fastställd som ett hjälpverktyg för näringsidkare, men är *per se* inte lagligt bindande. Lagen kräver åtgärder endast i de verksamheter som omfattar minst femhundra anställda i den egna verksamheten eller inom en koncern med ett moderbolag vars huvudkontor är placerat i Frankrike med minst femhundra anställda och där omsättningen är större än 100 miljoner euro. Stora företag kan därmed utföra tredjepartsbesiktning i förhållande till GDPR eftersom det krävs enligt *Sapin II*. Detsamma kan inte sägas om företag som ligger under anförda gränser. Det går eventuellt att argumentera för att en näringsidkare som vidtagit åtgärder enligt riktlinjerna för att förhindra och upptäcka korruption,

och därmed brutit mot GDPR möjligen skulle kunna få lägre böter eller, beroende på vilka säkerhetsåtgärder som vidtagits i förhållande till personuppgifterna, undgå sanktioner av den anledningen att kampen mot korruption får antas vara angelägen i Frankrike, se avsnitt 4.4.

5.3 Tredjepartsbesiktning i Sverige

5.3.1 Rättslig förpliktelse

Trots att Sverige har anslutit sig till diverse internationella regelverk för att motverka korruption är det tveksamt om Sverige har gjort tillräckligt för att leva upp till dessa. Senast i maj 2019 kritiserades Sverige för avsaknaden av en nationell strategi för att förebygga korruption. Det senaste krafttaget som gjordes inom lagstiftningens område specifikt för att förhindra korrupta betalningar i näringsverksamhet var när bestämmelsen om vårdslös finansiering av mutbrott infördes 2012. Bestämmelsen är problematisk eftersom brottet kräver ett begånget mutbrott. Det innebär till stor del att en tredjepartsbesiktning, för att undvika att fällas för vårdslös finansiering av mutbrott, kräver att verksamhetsutövaren ifråga i viss mån redan har vetskap om att mutbrottet har begåtts eller ska begås. Som Åklagarmyndigheten anförde i sitt remissvar innebär det i teorin att man istället gör sig skyldig till mutbrott, se avsnitt 4.1. Förmodligen blev bestämmelsen så svårtillämpad som vissa remissinstanser farhågade, eftersom brottet ännu inte tycks ha prövats i domstol.

Eftersom krav på personuppgiftsbehandling enligt tredje lands lag inte utgör en rättslig förpliktelse enligt GDPR är näringsidkare förhindrade att hänvisa till USA:s strikta antikorruptionsreglering för att genomföra tredjepartsbesiktning. *FCPA* skulle möjligen utgöra en laglig grund för att behandla personuppgifter och genomföra tredjepartsbesiktning om Sverige och USA ingick ett sådant avtal. Att reglera saken på nationell nivå i Sverige ligger förmodligen närmare till hands. Efterlevnad av *FCPA* kan dock omfattas av näringsidkarens intresse i enlighet med art. 6.1 f i GDPR. Eftersom bestämmelsen beskrivs som något av en slasktratt är det dock svårt

att avgöra vad som egentligen omfattas av undantaget och hur det ska tillämpas, se avsnitt 3.5.4.

Frågan är om bestämmelsen om vårdslös finansiering av mutbrott kan anses utgöra en rättslig förpliktelse i GDPR:s mening. Som beskrivet i avsnitt 3.5.4 krävs det enligt GDPR att syftet med den rättsliga förpliktelsen framgår, och att bestämmelsen inte får formuleras för ospecificerat eller svepande, resulterande i för stort handlingsutrymme för verksamhetsutövaren. Vad gäller undantag att behandla känsliga personuppgifter eller brottsuppgifter ställs högre krav på undantagsregelns specificering, se avsnitt 3.5.6 och 3.5.7.

I Sverige har det konstaterats tillräckligt att det allmänna intresset eller den rättsliga förpliktelsen regleras i bestämmelsen, utan att själva personuppgiftsbehandlingen uttryckligen framgår. Huruvida en rättslig förpliktelse föreligger eller ej kan också bedömas utifrån förarbeten och rättslig kontext, se avsnitt 3.5.4. Bestämmelsen om vårdslös finansiering av mutbrott kräver som beskrivet i avsnitt 4 grov oaktsamhet, och främjandet till mutbrottet ska utgöras av ett otillåtet risktagande vilket kan ske genom otillräckliga kontroll- eller försiktighetsåtgärder. Regeringen ansåg att bestämmelsen skulle ge incitament till kontroll av mellanhänder, till skillnad från några av remissinstanserna som var av motsatt uppfattning. Att propositionen dessutom nämner att Sveriges internationella åtaganden även inkluderar förebyggande arbete mot korruption kan tala för att bestämmelsen syftade till att åstadkomma en ökning av tredjepartsbesiktning, se avsnitt 4. Det finns alltså mycket som talar för att vårdslös finansiering av mutbrott kan anses utgöra en rättslig förpliktelse. Att bestämmelsen är opraktiskt utformad ur åtalssynpunkt torde inte ha någon betydelse vad gäller tillåtligheten att genomföra tredjepartsbesiktning, frågan är snarare om det är praktiskt möjligt att lagföra någon som inte uppvisar aktsamhet och underlåter att genomföra tillräckliga kontroll- och försiktighetsåtgärder. Datainspektionen har genom en särskild föreskrift tillåtit verksamhetsutövare att behandla brottsuppgifter gällande nyckelpersoner i företag i visselblåsarsystem med syftet att utreda oegentligheter, se avsnitt 3.5.7. Eftersom att föreskriften specifikt avser visselblåsarsystem finns det anledning att anta att Datainspektionen inte

tillåter behandling av brottsuppgifter utanför visselblåsarsystem, vilket med anledning av denna utredning möjligen kan ifrågasättas.

5.3.2 Möjliga åtgärder

Det finns vissa likheter mellan de åtgärdsförslag som räknas upp i propositionen till vårdslös finansiering av mutbrott och de vägledningar Frankrike, Storbritannien och USA uppvisar. Dessa är dock mycket mer utarbetade och detaljerade än åtgärdsförslagen i den svenska propositionen. Den typ av regelsystem som uppställer åtgärdsskyldighet av näringsidkare som används av USA, Frankrike och Storbritannien framstår som ett effektivt och konstruktivt system. En regering som av sina näringslivsaktörer kräver proaktivt arbete som förebyggande åtgärder mot korruption kommer förr eller senare, genom praxis eller riktlinjer, visa vilka typer av åtgärder som anses tillräckligt bra för att undvika korruption i sin verksamhet och därmed även lagföring. Det ger näringslivsaktörer goda förutsättningar att kunna bedriva en ren verksamhet som i längden visar sig mer lönsam än de aktörer som är inblandade i korruption. Förutom ekonomiska konsekvenser i form av böter och skadestånd drabbas korruptionsinblandade företag hårt av skadat anseende på marknaden. Ett regelsystem som eftersträvar förebyggandet av korruption ger lönsamma effekter både för samhället i stort och för den enskilda näringsidkaren. Det finns därmed god anledning för Sverige att utveckla och synliggöra tredjepartsbesiktning.

Vad gäller uppgifter om bidragsgivare till politiska partier är dessa att anse som känsliga personuppgifter då de avslöjar politisk tillhörighet, se avsnitt 3. Insynslagen bör i sig utgöra en rättslig förpliktelse till ett viktigt allmänt intresse, vilket omfattas av GDPR:s undantag. Men dataskyddslagen tycks ha minskat tillämpningsområdet för rekvisitet viktigt allmänt intresse i art. 9.2 i GDPR avsevärt till att endast omfatta myndigheter, se avsnitt 3.5.6. Vidare får uppgifterna bara behandlas om det krävs av en verksamhetsutövare i sin fullgörelse av rättigheter och skyldigheter inom arbetsrätten eller områden för hälsa och social trygghet, eller då individen har lämnat sitt samtycke. Syftet med lagen är att säkerställa öppenhet och transparens kring vilka intressen

som står bakom politiska partiers finansiering för att motverka korruption, varpå verksamhetsutövare borde berättigas inhämtning av sådan information för att använda i sin tredjepartsbesiktning.

Datainspektionen har fått stora befogenheter att utfärda både allmänna föreskrifter och enskilda tillstånd till verksamhetsutövare, se avsnitt 3. Även om det många gånger ur ett förutsebarhetsperspektiv är önskvärt med en detaljerad lag över tillåtna undantag, har dagens lösning vissa fördelar. Datainspektionens befogenheter kan genom förarbetena tolkas som en skyldighet för myndigheten att hålla sig uppdaterad om regleringens utveckling och dess konsekvenser. Lösningen kan ha ansetts vara den bästa då konsekvenserna av GDPR var mycket osäkra, varpå ett dynamiskt regelsystem kan vara fördelaktigt jämfört med utdragna lagstiftningsprocesser som varje nyuppkommet problem skulle kunna medföra. Även GDPR fastslår tillsynsmyndighetens skyldighet att hålla sig uppdaterad inom områdets utveckling i samhället, se avsnitt 3.5. Upplägget att Datainspektionen kan ge enskilda tillstånd för behandling av brottsuppgifter framstår dock som något opraktisk ut belastningssynpunkt. Att upprätta generella föreskrifter som samtliga verksamhetsutövare istället kan ta del av är en desto effektivare lösning. En sådan föreskrift skulle i likhet med Irlands regelverk kunna innehålla tillåtlighet att behandla brottsuppgifter och känsliga personuppgifter för uppfyllandet av vårdslös finansiering av mutbrott och andra för antikorruptionsarbete relevanta bestämmelser, se avsnitt 4.2.

En alternativ lösning är att frågan regleras i kollektivavtal, eftersom kollektivavtal anses utgöra en rättslig grund, se avsnitt 3.5.4 och 3.5.6. Eventuellt omfattas även kollektivavtalet av Datainspektionens föreskrift om tillåtna undantag för brottsuppgiftsbehandling inom arbetsrätten. Det är dock inte en ultimat lösning, eftersom det inte står helt klart under vilka omständigheter eller hur vidsträckt betydelse kollektivavtalet får, se avsnitt 3.5.1.

Ur ett långsiktigt perspektiv bör regeringen upprätta bestämmelser som i likhet med de regelverk som upprättats i bland annat USA, Frankrike och Storbritannien vilka på ett tydligt sätt kräver specifika åtgärder för att förebygga korruption i näringsverksamhet. Detta kan göras sedvanligt genom lag, alternativt genom hänvisning till Institutet Mot Mutors Näringslivskod och dess funktion som näringslivets självreglering, jämför med till exempel Kollegiet för svensk bolagsstyrning. Institutet Mot Mutors uppdrag att förvalta självregleringen för att undvika mutbrott i sin verksamhet skulle därmed kunna utvidgas i likhet med *AFA Guidelines*, *FCPA Guide* och *The U.K Bribery Act Guidance*.

Det är tydligt att nämnda länders regelverk i dess proaktiva anda gör det lättare för verksamhetsutövare att följa samt förstå regelverket, till skillnad från Sveriges snarare reaktiva bestämmelser. Bestämmelserna måste också vara flexibla på så sätt att verksamhetsutövare tillåts att följa regelverket utifrån vad som är lämpligt i förhållande till sin egna verksamhet samt vid bedömning av lämpliga sanktioner, snarare än att tillämpa statiska verkställighetsåtgärder, se till exempel avsnitt 4.4.2. Ett effektivt system förutsätter också att efterlevnad av åtgärdskraven måste stå sig ekonomiskt fördelaktig i förhållande till de ekonomiska konsekvenserna som ett regelbrott kan medföra, och på så sätt ge incitament för förebyggande arbete. Vad ett svenskt regelverk mer specifikt bör innehålla är en utredning för sig, men klart är att det i alla fall bör påkalla både interna och externa riskbedömningar som inkluderar tredjepartsbesiktning. Det bör också framgå exempel på åtgärder som kan vidtas för att genomföra tredjepartsbesiktning, något som USA, Frankrike och Storbritannien samtliga exemplifierar på ett ypperligt sätt.

Käll- och litteraturförteckning

Tryckta källor

Sverige

Propositioner

Prop. 2000/01:105 *Förbud mot juridiskt eller ekonomiskt biträde i vissa fall.*

Prop. 2011/12:79 *En reformerad mutbrottslagstiftning.*

Prop. 2013/14:70 *Ökad insyn i partiers och valkandidaters finansiering*.

Prop. 2017/18:55 *Ökad insyn i partiers finansiering – ett utbyggt regelverk.*

Prop. 2017/18:95 *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning.*

Prop. 2017/18:105 *Ny dataskyddslag.*

Statens Offentliga utredningar

SOU 1997:39 *Integritet Offentlighet Informationsteknik.*

SOU 1999:109 *Behandling av personuppgifter inom socialtjänsten.*

SOU 2001:32 *Domstolarnas register och personuppgiftslagen – En rättslig anpassning.*

SOU 2001:100 *Informationshantering och behandling av uppgifter vid domstolar – En rättslig översyn.*

SOU 2009:44 *Integritetsskydd i arbetslivet.*

SOU 2010:38 *Mutbrott*

SOU 2017:39 *Ny dataskyddslag.*

Kommittédirektiv

Kommittédirektiv 2016:15 *Dataskyddsförordningen.*

Departementspromemoria

Ds 2013:31 *Allmänhetens insyn i partiers och valkandidaters finansiering.*

Datainspektionens författningssamling

DIFS 2018:2 *Föreskrifter om behandling av personuppgifter som rör lagöverträdelser*.

Europeiska Unionen

Artikel 29-gruppen: *Yttrande 6/2014 om begreppet registeransvariges berättigade intressen enligt artikel 7 direktiv 95/46/EG.* 3284/16/EN WP 217. Bryssel 2016. *Citeras Artikel 29-gruppens yttrande 6/2014.*

Europeiska kommissionen: *Rapport från kommissionen till Rådet och Europaparlamentet EU:s rapport om insatserna mot korruption*. COM (2014) 38 final. Bryssel 2014. Svensk version. *Citeras EU:s rapport om insatserna mot korruption.*

Europeiska kommissionen*: Rapport från kommissionen till Rådet och Europaparlamentet COM (2014) 38 final Annex 27 Bilaga Sverige till EU:s rapport om insatserna mot korruption*. Bryssel 2014. Svensk version. *Citeras EU:s rapport om insatserna mot korruption, Annex 27, Bilaga Sverige.*

Sveriges ständiga representation vid Europeiska unionen Bryssel: *D-post: BRYR/2016-05-01/1503*. Bryssel 2016. *Citeras D-post: BRYR/2016-05-01/1503.*

GRECO: *Fifth evaluation round Preventing corruption and promoting integrity in central governments (top executive functions) and law enforcement agencies, Evaluation report Sweden.* GrecoEval5Rep(2018)4. Publicerad 2019-05-03. *Citeras GRECO, Evaluation report Sweden.*

Statliga riktlinjer

Frankrike

Agence Francaise Anticorruption: *Guidelines to help private and public sector entities prevent and detect corruption, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favouritism*. Version 12-2017. *Citeras AFA Guidelines*.

USA

Criminal Division of the U.S. Departement of Justice, Enforcement Division of the U.S. Securities and Exchange Commission: *FCPA A resource Guide to the U.S. Foreign Corrupt Practices Act*. 2012. *Citeras FCPA Guide.*

UK

Ministry of Justice: *The Bribery Act 2010 Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing*. 2010. *Citeras The U.K Bribery Act Guidance.*

Litteratur

Beyer; Sandra, Edvardsson; Tobias, Frydlinger; David, Olstedt Carlström; Caroline: *GDPR Juridik, organisation och säkerhet enligt dataskyddsförordningen.* Första upplagan. Stockholm 2018. *Citeras Frydlinger m.fl.*

Borglund; Tommy, De Geer; Hans, Sweet; Susanne; Frostensson; Magnus, Lerpold; Lin, Nordbrand; Sara, Sjöström; Emma, Widell; Karolina: *CSR och hållbart företagande*. Andra upplagan. Stockholm 2017. *Citeras Borglund m.fl.*

Cars; Thorsten: *Mutbrott och korruptiv marknadsföring*. Tredje upplagan. Stockholm 2012. Citeras *Cars.*

Friberg; Sandra: *Brottsbalk (1962:700) 10 kap. 5 e §,* Lexino 2017-09-02. *Citeras Friberg.*

Kleineman; Jan: *Rättsdogmatisk metod*, i: Nääv; Maria, Zamboni; Mauro (red.): *Juridisk Metodlära*. Andra upplagan. Lund 2018. *Citeras Kleineman*.

Oded; Sharon: Corporate Compliance New Approaches to Regulatory Enforcement. Massachusettes, USA, 2013. *Citeras Oded*.

Reichel; Jane: *EU-rättslig metod*, i: Nääv; Maria, Zamboni; Mauro (red.): *Juridisk Metodlära*. Andra upplagan. Lund 2018. *Citeras Reichel*.

Sandgren; Claes: *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*. Fjärde upplagan. Stockholm 2018. *Citeras Sandgren (2018).*

Sandgren; Claes: *Rättsanalytisk metod. En väg framåt?,* i: Karnell, Gunnar (red.), *Liber Amicorum Jan Rosén*. Visby 2016. *Citeras Sandgren (2016).*

Sundstrand; Andrea: *Offentlig upphandling och korruption*. Juridisk Tidsskrift nr 1 2014/15. *Citeras Sundstrand*.

Valguarnera; Filippo: *Komparativ juridisk metod*, i: Nääv; Maria, Zamboni; Mauro (red.): *Juridisk Metodlära*. Andra upplagan. Lund 2018. *Citeras Valguarnera*.

Wendleby; Monika, Wetterberg; Dag: Dataskyddsförordningen GDPR, Förstå och tillämpa i praktiken. Andra upplagan. Stockholm 2019. *Citeras Wendleby & Wetterberg*.

Öman; Sören: *Dataskyddsförordningen (GDPR) m.m*. *En kommentar.* Upplaga 1:1. Stockholm 2019. *Citeras Öman*.

Referenslitteratur

Trolle Önnerfors; Elsa, Wenander; Henrik: *Att skriva rätt Goda råd för att skriva uppsats i juridik*. Andra upplagan. Stockholm 2019.

Övrigt

Standarder

ISO 37001:2016 *Anti-bribery management systems- Requirements with guidance for use.*

Beslut och yttranden
Datainspektionens yttrande 2007-05-25, dnr 1036-2006
Datainspektionens beslut 2015-10-15 dnr 1382-2014.

Remissvar
Dnr Ju2010/4890/L5 *Yttrande mutbrott*, Sveriges Domstolar.
<www.domstol.se/Publikationer/Remisser/2010/1231-2010%20Yttrande%20Mutbrott.pdf> (hämtad 2019-08-06).

Dnr EBM A-2010/0318 *Yttrande mutbrott*, Ekobrottsmyndigheten.
<www.ekobrottsmyndigheten.se/Documents/Remisser_yttranden/Remissvar%202010/Ju_2010_38_Mutbrott.pdf> (hämtad 2019-08-06).

Dnr ÅM-A 2010/1097 *Yttrande över betänkandet ”mutbrott” (SOU 2010:38),* Åklagarmyndigheten.

Elektroniska källor

Standarder och konventioner
ICC *Rules on Combating Corruption*.
<www.cdn.iccwbo.org/content/uploads/sites/3/2011/10/ICC-Rules-on-Combating-Corruption-2011.pdf> (hämtad 2019-08-06).

OECD *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*, 17 December 1997.
<www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf>
(hämtad 2019-08-06).

OECD *Convention on the Organisation for Economic Co-operation and Development*, Paris 14th December 1960.
<www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm> (hämtad 2019-08-06).

OECD *Guidelines for Multinational Enterprises*, 2011 edition.
<www.oecd.org/daf/inv/mne/MNEguidelinesSVENSKA.pdf>

(hämtad 2019-08-06).

OECD *Due Diligence Guidance for Responsible Business Conduct*, 31 May 2018. <www.mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf> (hämtad 2019-08-06).

United Nations *Convention against Corruption* General Assembly resolution 58/4 of 31 October 2003. <www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf> (hämtad 2019-08-06).

Undersökningar
Corruption Perception Index 2018, Transparency International <www.transparency.org/cpi2018> (besökt 2019-08-06).
<www.transparency.org/cpi2018#results> (besökt 2019-08-06).

Artiklar och reportage
Dagens Nyheter: publicerad 2019-02-27. <www.dn.se/ekonomi/korruptionsexpert-swedbank-riskerar-att-utestangas-fran-internationell-handel/> (besökt 2019-08-06).

Omni <www.omni.se/utredning-om-mutbrott-pa-trafikverket-i-umea/a/kaR7ok> (besökt 2019-08-06).

SvD Näringsliv: Alestig; Peter, Vanhainen; Ida, publicerad 2018-12-18. <www.svd.se/telias-mutharva-i-uzbekistan-detta-har-hant-xycx> (besökt 2019-08-06).

Svenska Dagbladet: publicerad 2017-11-13. <www.svd.se/vagmalare-vittnar-om-mutor-pa-trafikverket> (besökt 2019-08-06).

Svenska Dagbladet: Gummesson; Jonas, publicerad 2017-11-30.

<www.svd.se/saab-anmals-for-mutbrott--hogsta-cheferna-kan-forhoras>
(besökt 2019-08-06).
Sveriges Radio: P3 Dokumentär, ansvarig utgivare Diljen; Silan, publicerad 2018-10-14.
<www.sverigesradio.se/sida/avsnitt/1174260?programid=2519>
(besökt 2019-08-06).

SVT Nyheter: Schützer; Karolina, publicerad 2017-03-09.
<www.svt.se/nyheter/inrikes/korruptionsskandalen-pa-statensfastighetsverk-detta-har-hant> (besökt 2019-08-06).

SVT Nyheter: ansvarig utgivare Johansson; Ulf, publicerad 2019-02-20.
<www.svt.se/special/swedbank/> (besökt 2019-08-06).

Systembolaget: pressmeddelande, publicerat 2012-02-23.
<www.press.systembolaget.se/systembolaget-fortsatter-bekampakorruption-trots-skadestand-i-ny-dom/> (2019-08-06).

UN News: publicerad 2018-12-09.
<www.news.un.org/en/story/2018/12/1027971> (besökt 2019-08-06).

World Economic Forum: publicerad 2018-12-13.
<www.weforum.org/agenda/2018/12/the-global-economy-loses-3-6-trillion-to-corruption-each-year-says-u-n/> (besökt 2019-08-06).

Övriga internetkällor

Datainspektionen:
<www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/personuppgifter-som-ror-lagovertradelser/>
(besökt 2019-08-07).

Europeiska dataskyddsstyrelsen:
<www.edpb.europa.eu/edpb_sv> (besökt 2019-09-02).

GRECO:
<www.coe.int/en/web/greco/about-greco/priority-for-the-coe>
(besökt 2019-08-06).

Institutet Mot Mutor:
<www.institutetmotmutor.se/kunskapsbank/ordlista/korruption/>
(besökt 2019-08-06).

Nationalencyklopedin:
<www.ne.se/uppslagsverk/encyklopedi/lång/korruption>
(besökt 2019-08-06).

OECD:
<www.oecd.org/cleangovbiz/49693613.pdf> (besökt 2019-08-06).

Svenska Akademin:
<www.svenska.se/tre/?sok=korruption&pz=1> (besökt 2019-08-06).

Transparency International:
<www.transparency.se/korruption> (besökt 2019-08-06).

World Economic Forum:
<www.reports.weforum.org/global-agenda-council-2012/councils/anti-corruption/> (besökt 2019-08-06).

Rättsfallsförteckning

Sverige
Stockholms tingsrätts dom 2019-02-15 i mål nr B 122201–17.
Umeå tingsrätts dom 2019-02-21 i mål nr B 2793–17.
Hovrätten för Västra Sveriges dom 2018-02-06 i mål nr B 2742–17.

EU
EU:C:2003:596 C-101/01 Lindqvist.
ECLI:EU:C:2008:724 Domstolens dom (stora avdelningen) den 16 december 2008, C-524/06 Heinz Huber v Bundesrepublik Deutschland.