



EKONOMI-  
HÖGSKOLAN

# Penningtvättslagen och dataskyddsförordningen - förhåller de sig till varandra?

En studie om sambandet mellan regleringarna  
om penningtvätt och dataskyddsrätt

**Johanna Hansson**

INSTITUTIONEN FÖR HANDELSRÄTT

Affärsjuridisk kandidatuppsats

15 högskolepoäng

HARH13

VT 2024



# Sammanfattning

Syftet med uppsatsen är att beskriva och analysera förhållandet mellan bestämmelser om penningtvätt och dataskyddsrätt, med fokus på huruvida företags förpliktelser enligt penningtvättslagen påverkas av reglerna i dataskyddsförordningen.

Den tekniska utvecklingen har bidragit inte bara till att underlätta för individer och företag utan också för den ekonomiska brottligheten. Genom utnyttjande av moderna tekniska lösningar och tjänster, samt ett regelverk som inte hängt med den digitala utvecklingen, kan kriminella genomföra olika ekonomiska brott på en nationell såväl som en internationell nivå. För att motverka den ekonomiska brottligheten finns regleringar och samarbeten på internationell, europeisk och nationell nivå.

Arbetsgruppen för finansiella åtgärder (FATF) är en internationell organisation som utfärdar rekommendationer för att främja arbetet mot penningtvätt. Dessa rekommendationer har EU i sin tur valt att basera sina penningtvättsdirektiv på, och som i sin tur är införlivat i lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). Regleringarna innehåller diverse åtgärder för verksamhetsutövare att vidta för att motverka penningtvätt. En central del i det arbetet är kundkännedomprocessen. Vid kundkännedomprocessen inhämtar verksamhetsutövare data genom att ställa frågor till kunden för att förstå syftet med affärsförbindelsen och transaktionerna. Då processen innefattar behandling av personuppgifter blir den allmänna dataskyddsförordningen aktuell.

Av uppsatsens resultat framgår det att verksamhetsutövare måste uppfylla kraven i dataskyddsförordningen vid behandling av personuppgifter. Nuvarande lagstiftning pekar enbart på viss enlighet mellan regelverken men det förväntas lösas med regelverk på penningtvättsområdet. Genom de nya regelverken är förhoppning att större hänsyn tas till kundens rättigheter och friheter. För närvarande ska penningtvättslagstiftningen läsas i ljuset av dataskyddsförordningen, med hänsyn till ökad öppenhet och skydd för personlig integritet.

**Ämnesord:** allmänna dataskyddsförordningen, ekonomisk brottlighet, kundkännedom, penningtvätt, verksamhetsutövare.

# Abstract

The purpose of the thesis is to describe and analyse the relationship between regulations on money laundering and data protection law, with a focus on whether companies' obligations under the Money Laundering Act are affected by the rules in the data protection regulation.

Technological developments have contributed not only to making it easier for individuals and companies, but also for financial crime. Making full use of modern technical solutions and services, as well as a regulatory framework that has not kept up with digital developments, criminals can carry out various financial crimes on a national as well as an international level. To counter economic crime, there are regulations and collaborations at international, European and national level.

The Financial Action Task Force (FATF) is an international organization that issued recommendations to promote anti-money laundering work. The EU has in turn chosen to base its money laundering directives on these recommendations, which in turn are incorporated into law (2017:630) on measures against money laundering and financing of terrorism (the Money Laundering Act). The regulations contain various measures for operators to take to counter money laundering. A central part of that work is the customer awareness process. In the customer due diligence process, operators gather data by asking the customer questions to understand the purpose of the business relationship and transactions. As the process includes the processing of personal data, the General Data Protection Regulation becomes relevant.

From the results of the thesis, it appears that operators must meet the requirements of the data protection regulation when processing personal data. Current legislation only points to some conformity between the regulations, but it is expected to be solved with new money laundering regulations. Through the new regulations, it is hoped that greater consideration will be given to the customer's rights and freedoms. Currently, the money laundering legislation must be read in the light of the data protection regulation, considering increased transparency and protection of personal privacy.

**Keywords:** business operators, customer awareness, financial crime, General Data Protection Regulation, money laundering.

# Innehåll

<b>Sammanfattning .....</b>	<b>3</b>
<b>Förkortningar .....</b>	<b>7</b>
<b>1 Inledning.....</b>	<b>9</b>
1.1 Bakgrund .....	9
1.2 Syfte och frågeställningar.....	10
1.3 Avgränsningar .....	11
1.4 Metod och material.....	11
1.5 Disposition .....	12
<b>2 Penningtvätt .....</b>	<b>13</b>
2.1 Vad är penningtvätt? .....	13
2.2 Internationella riktlinjer för bekämpande av penningtvätt.....	13
2.3 Europeiska unionens penningtvättsdirektiv .....	14
2.3.1 EU:s nuvarande penningtvättsdirektiv .....	14
2.3.2 EU:s förslag till nya åtgärder för penningtvätt.....	15
2.4 Nationell lagstiftning gällande penningtvätt .....	17
2.5 Kundkännedom enligt penningtvättslagen.....	17
2.5.1 Varför behövs kundkännedom? .....	17
2.5.2 Åtgärder för kundkännedom .....	18
2.5.3 Samspelet mellan kundkännedom, riskbedömning och övervakning .....	20
<b>3 Behandling av personuppgifter vid kundkännedom.....</b>	<b>22</b>
3.1 Grundläggande om dataskyddsförordningen .....	22
3.1.1 Syftet med dataskyddsförordningen.....	22
3.1.2 Personuppgiftsbegreppet .....	22
3.1.3 Materiellt och territoriellt tillämpningsområde .....	23
3.2 Rättslig grund för behandling av personuppgifter.....	24
3.2.1 Rättslig grund .....	24
3.2.2 Stark rättslig grund.....	25
3.2.3 Svag rättslig grund .....	26
3.2.4 Lagöverträdelse .....	27
3.3 Insamling och lagring av personuppgifter.....	28
3.3.1 Uppgiftsminimering .....	28
3.3.2 Lagringsminimering.....	28
3.4 Informationsskyldighet gentemot den registrerade .....	29
<b>4 Samspelet mellan dataskyddsförordningen och penningtvättslagen.....</b>	<b>31</b>
4.1 Allmänt om samspelet.....	31
4.2 Samverkan i förhållande till bestämmelserna i dataskyddsförordningen.....	32
4.3 Förhållandet mellan dataskyddsförordningen och förslaget till ny penninglagstiftning.....	33
4.3.1 Förordningsförslagets samspel med dataskyddsförordningen .....	33
4.3.2 Direktivförslagets samspel med dataskyddsförordningen.....	34

<b>5 Avslutande diskussion .....</b>	<b>36</b>
<b>Källförteckning .....</b>	<b>39</b>

# Förkortningar

AML	Anti-Money laundering (penningtvätt)
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheter och de grundläggande friheterna
EU	Europeiska unionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
FATF	Arbetsgruppen för finansiella åtgärder
FEUF	Fördraget om Europeiska unionens funktionssätt
FN	Förenta nationerna
GDPR	Allmänna Dataskyddsförordningen
IMF	Internationella valutafonden
IMY	Integritetsmyndigheten
PEP	Politisk utsatt ställning
SFS	Svensk författningssamling
SOU	Statens offentliga utredningar





# 1 Inledning

## 1.1 Bakgrund

Varje år uppgår penningtvätten i världen till ett estimerat värde på 2-5% av den års-globala bruttonationalprodukten (BNP) vilket motsvarar mellan 715 miljarder och 1.87 biljoner euro.<sup>1</sup> Sverige är inget undantag utan enligt rapporten “Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2019” uppskattas att cirka 130 miljarder SEK tvättas genom det svenska finansiella systemet varje år.<sup>2</sup> Allt oftare har penningtvättbrott internationella kopplingar och i takt med att dessa ökar blir brotten också allt grövre. Kriminella verkar alltmer globalt och använder länder vars finansiella system har luckor som möjliggör penningtvätt.<sup>3</sup> Penningtvätt förekommer i samband med olagliga aktiviteter såsom smuggling, förskingring, insiderbrott, försäljning av vapen, mutbrott och datorbedrägerier. Det är även vanligt förekommande inom den organiserade brottslighetens handel med människor (inklusive prostitution), vapen och droger.<sup>4</sup>

Genom digitaliseringen av samhället skapas nya möjligheter för den organiserade ekonomiska brottsligheten. Brottsligheten lutar sig alltmer mot moderna tekniska lösningar och tjänster, och skapar ökade möjligheter att undvika upptäckt under planering och genomförande av olika former av ekonomiska brott. Efter hand som utbudet av finansiella betaltjänster ökar underlättar det för organiserade brottslingars möjlighet att genomföra internationella penningtvättsupplägg. För att bekämpa ekobrotten behöver lagstiftningen vara anpassad till den digitala utvecklingen.<sup>5</sup>

Den svenska penningtvättslagstiftningen syftar till att förhindra att företag utnyttjas för penningtvätt och terrorfinansiering.<sup>6</sup> För att kunna försvåra penningtvätt måste företag ha god kundkännedom och göra en riskbedömning av kunden. Utan tillräcklig kundkännedom får inte företaget etablera eller behålla en affärsrelation, eller utföra enstaka transaktioner. Detsamma gäller om ett företag misstänker att deras produkter och tjänster kan komma att användas för penningtvätt eller finansiering av terrorism.<sup>7</sup> Banker, försäkringsbolag och andra finansiella företag ska göra en bedömning av risken för att de produkter och tjänster som de erbjuder utnyttjas för penningtvätt eller finansiering av terrorism samt hur stor den risken är. Riskbedömningen ska innehålla typ av produkter och tjänster som erbjuds, kunder och distributionskanaler samt geografiska riskfaktorer.<sup>8</sup> Banker och annan finansiell

---

<sup>1</sup> Europol, *Money Laundering*, u.å.

<sup>2</sup> Ekobrottsmyndigheten, *Penningtvättsbrott*, u.å.

<sup>3</sup> Ibid.

<sup>4</sup> Sas institute, *Penningtvätt: Vad är AML och varför är det viktigt*, u.å.

<sup>5</sup> Ekobrottsmyndigheten, *EBM:s lägesbild om ekonomisk brottslighet i Sverige*, 2021.

<sup>6</sup> Finansinspektionen, *Penningtvätt*, 2023.

<sup>7</sup> Finansinspektionen, *Kundkännedom*, 2023.

<sup>8</sup> Finansinspektionen, *Riskbedömning*, 2024.

verksamhet har en särskilt hög inneboende risk för penningtvätt och kan även ha stora samhällskonsekvenser.<sup>9</sup>

Trots att Sverige generellt håller en god nivå vad gäller arbete med bekämpning av penningtvätt och terrorfinansiering kvarstår ett flertal utmaningar fortfarande. Ekobrottsmyndigheten har bland annat identifierat systemriskerna kopplade till målvakter, folkbokföring och utnyttjade identiteter. Utöver det har även brister på resurser och verktyg samt tillräckligt lagstöd för vissa områden uppmärksamats.<sup>10</sup>

När företag bygger upp sin kundkänedom behandlar de personuppgifter. Hur personuppgifter ska hanteras bestäms i den allmänna dataskyddsförordningen, mer känd som GDPR vilket är förkortningen av förordningens engelska namn General Data Protection Regulation. I skäl 65 i fjärde penningtvättsdirektivet framgår att direktivet är förenligt med de grundläggande rättigheter som fastställs i Europeiska unionens stadga om de grundläggande rättigheterna, framför allt med fokus på rätten till privatliv och skydd av personuppgifter.<sup>11</sup> Skyddet av personuppgifter som rör en fysisk person föreskrivs i både stadgan och i fördraget om Europeiska unionens funktionssätt (FEUF). GDPR innehåller regler som principerna om lagringsminimering och uppgiftsminimering (artikel 4.1 led c och e). Det innebär att uppgifter som samlas in ska vara "adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas",<sup>12</sup> och sedan inte får "förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas."<sup>13</sup> Det finns även regler i artikel 10 GDPR gällande behandling av personuppgifter som rör fällande domar i brottmål samt lagöverträdelse som innefattar brott samt vem som får kontrollera och behandla dem.

## 1.2 Syfte och frågeställningar

Syftet med den här uppsatsen är att beskriva och analysera förhållandet mellan bestämmelser om penningtvätt och dataskyddsrätt, med fokus på huruvida företags förpliktelser enligt lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism påverkas av reglerna i dataskyddsförordningen.

- *Vilka skyldigheter åläggs verksamhetsutövare vid insamling och behandling av kunddata för att uppnå kundkänedom enligt penningtvättslagstiftningen?*
- *Vilka krav ställs på verksamhetsutövare enligt EU:s dataskyddsförordning när personuppgifter behandlas för att uppnå en god kundkänedom i samband med bekämpning av penningtvätt?*

---

<sup>9</sup> Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s.6.

<sup>10</sup> Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s.10.

<sup>11</sup> Skäl 65, Direktiv 2015/849.

<sup>12</sup> Artikel 4.1 led c i GDPR.

<sup>13</sup> Artikel 4.1 led e i GDPR.

### 1.3 Avgränsningar

Uppsatsen ägnar sig åt att undersöka ovannämnda frågeställning med fokus på verksamhetsutövare i penningtvättslagens mening och hur deras penningtvätsarbete påverkas av dataskyddsförordningen. I uppsatsen är straffrättsliga bestämmelser med avseende på penningtvätt inte ett fokus och kommer därför att exkluderas. Det innebär att bestämmelser såsom lag (2014:307) om straff för penningtvätsbrott eller brottsdatalogen (2018:1177) inte kommer att behandlas i uppsatsen.

Vidare kommer uppsatsen främst behandla regelverk på europeisk och nationell svensk nivå, men kommer även översiktligt behandla internationellt riktlinjer för penningtvätt på grund av dess påverkan på EU:s penningtvätsdirektiv. Fokus ligger främst på nuvarande lagstiftning men kommer även ha ett fokus på EU:s nya åtgärds paket för AML.

### 1.4 Metod och material

För att besvara frågeställningen kommer en rättsdogmatisk metod så väl som en EU-rättslig metod användas. En rättsdogmatisk metod bygger på att analysera de olika elementen i rättskällaläran så att resultatet speglar gällande rätt, och hur rättsregeln ska uppfattas i ett visst konkret sammanhang.<sup>14</sup> Källorna kommer att undersökas utifrån rättskällaläran och deras rättsliga dignitet. För uppsatsen är svensk lagstiftning av central betydelse. För att förstå och tillämpa lagstiftningen kommer förarbeten användas. Förarbeten är ett samlingsnamn för propositioner, utredningar, betänkanden, författningskommentarer och motiveringar som utarbetas under lagstiftningsförloppet.<sup>15</sup> Vidare är rättspraxis en rättskälla som används för att tolka lagstiftningen och gäller främst rättsliga avgörande från domstolar.<sup>16</sup> I uppsatsen kommer riktlinjer och tillsynsbeslut från myndigheter att användas då det finns en avsaknad av rättspraxis från EU-domstolen och svensk överdomstol på området.

EU-rättslig metod kommer användas då regler om penningtvätt och dataskydd har sitt ursprung i EU-rätten genom direktiv och förordning. Förordningar, direktiv och beslut från EU tillhör sekundärrätten, vanligen benämnt rättsakter.<sup>17</sup> Förordningar är allmänt tillämpliga i hela unionen enligt artikel 288.2 FEUF. Det innebär att EU-förordningarna är direkt tillämpliga och bindande i varje medlemsland. Det innebär att svenska myndigheter och domstolar ska tillämpa bestämmelserna utan att dessa behöver införlivas i nationell rätt. Direktiven ska däremot införlivas i nationell rätt genom lagstiftning enligt artikel 288.3 FEUF då de riktar sig till medlemsstaterna och inte till enskilda. Detta innebär att medlemsstaterna själva får bestämma form och tillvägagångsätt för genomförandet men är bundna vad gäller resultatet som ska uppnås.<sup>18</sup>

---

<sup>14</sup> Se Nääv, Maria & Zamboin, Mauro (red.) *Juridisk metodlära*. 2:3. Uppl. Lund: Studentlitteratur, 2021.

<sup>15</sup> Se Bernitz, Ulf, Carlsson, Mia, Heuman, Lars, Leijonhufvud, Madeleine, Magnusson Sjöberg, Cecilia, Seipel, Peter, Warnling Conradson, Wiweka och Vogel, Hans-Heinrich. *Finna rätt*. 15.1. uppl. Stockholm: Norstedts Juridik, 2020. s. 30–32, s. 125.

<sup>16</sup> *Ibid.*, s.155.

<sup>17</sup> *Ibid.*, s. 68.

<sup>18</sup> *Ibid.*, s. 68-69.

EU-rätten lägger stor vikt vid rättspraxis som utvecklats av EU-domstolen. Även om ett avgörande i EU-domstolen formellt sett endast är bindande i det konkreta fallet är det mycket ovanligt att domstolen frångår sin praxis och det är vanligt att de hänvisar till sina tidigare domar och bygger vidare på dem i nya avgöranden. EU-domstolen har en mer rättsskapande funktion än vad som varit normen i svensk rätt.<sup>19</sup> I uppsatsen tas ett mål från EU-domstolen upp men avsaknaden av rättsfall på området är märkbar även på EU-nivå.

## 1.5 Disposition

Uppsatsen är disponerad enligt följande ordning: Första kapitlet innehåller det inledande kapitlet med bakgrund, syfte och frågeställning, avgränsning, metod och material samt disposition. Det andra kapitlet i uppsatsen redogör för penningtvättslagstiftningen. Kapitlet börjar med en introduktion till penningtvätt och därefter hur reglerna på internationell, europeisk och nationell nivå i Sverige ser ut. Redogörelsen av den europeiska regleringen innehåller även ett avsnitt om nya regler som ska införas på området. Efter det kommer en redogörelse för hur reglerna kring kundkännedom ser ut enligt och vilka återgår som ska vidtas enligt penningtvättslagstiftningen för att motverka penningtvätt. I det tredje kapitlet beskrivs dataskyddsförordningen och behandling av personuppgifter. Först ges en beskrivning av förordningens syfte och tillämpningsområde. Det följs av vilka rättsliga grunder som är lämpliga att använda vid arbetet mot penningtvätt, hur uppgifter om lagöverträdelse får behandlas samt verksamhetsutövare informationsskyldighet mot kund. I det fjärde kapitlet redogörs samspelet mellan penningtvättslagen och dataskyddsförordningen, och hur samverkan får fungera mellan verksamhetsutövare och myndighet. Det fjärde kapitlet avslutas med att redogöra för hur den nya lagstiftningen förhåller sig till dataskyddsförordningen. I uppsatsens femte och avslutande kapitel diskuteras och analyseras resultatet av kapitel två, tre och fyra för att besvara uppsatsens frågeställning.

---

<sup>19</sup> Ibid, s. 73.

## 2 Penningtvätt

### 2.1 Vad är penningtvätt?

Vid penningtvätt används det finansiella systemet för illegala ändamål för att dölja en vinstgenererande brottslig handling.<sup>20</sup> De svenska reglerna på området grundas på ett antal penningtvättsdirektiv från Europeiska unionen (EU) som i sin tur bygger på rekommendationer från arbetsgruppen för finansiella åtgärder (FATF).

Penningtvätt är processen när kriminella döljer vinsten av sin kriminella verksamhet, ofta i form av kontanter, för att sedan kunna redovisa dem lagligt.<sup>21</sup> Genom att sopa igen spåren mellan brott och pengarna genom att tvätta dem kan kriminella dölja deras ursprung. Dagens penningtvättsbrott begås på en rad olika sätt såsom att någon förvarar eller transporterar kontanter för någon annans räkning eller använder sig av andra personers konton (så kallade målvakter). Utöver det finns även mer avancerade upplägg där pengarna flyttas runt i det finansiella systemet genom flera transaktioner i syfte att göra det svårt att följa dem. Det finns också så kallad självtvätt där gärningspersonen tvättar pengar från egen brottslighet genom att till exempel visa upp falska handlingar om pengarnas ursprung för att kunna sätta in dem på ett eget bankkonto. Begås penningtvätten inom en näringsverksamhet eller i större skala kan det vara fråga om näringspenningtvätt. En person kan dömas för näringspenningtvätt även om det senare visar sig att pengarna kom från legal verksamhet, då även klandervärt risktagande är brottsligt.<sup>22</sup> Penningtvätt kan därmed göras på olika sätt och med olika antal personer inblandade. Penningtvätt är ofta även kopplad till annan olaglig och organiserad brottslighet men även till finansiering av terrorism. Genom att spåra pengarna spåras samtidigt de kriminella nätverken.<sup>23</sup>

### 2.2 Internationella riktlinjer för bekämpande av penningtvätt

FATF, som bildades av G7-länderna<sup>24</sup>, arbetar med att ta fram internationella standarder för att motverka penningtvätt och bekämpa finansiering av terrorism. Sverige har varit medlem i FATF sedan dess grundande och även EU-kommission är i dag medlem. FATF:s 40 rekommendationer har spridit sig till 180 jurisdiktioner och organisationer som Förenta nationerna (FN), Internationella valutafonden (IMF) och Världsbanken har ställt sig bakom dessa rekommendationer. Organisationens arbete innefattar att säkerställa att dess rekommendationer får global spridning och efterlevs på ett effektivt sätt genom bland annat återkommande ömsesidiga utvärderingar av medlemsländernas system. De har även möjlighet att utfärda rekommendationer om åtgärder för medlemsländer som brister i sina system för

---

<sup>20</sup> Betänkande 2019/20: FiU15: Skärpta åtgärder mot penningtvätt och finansiering av terrorism.

<sup>21</sup> Europol, *Money Laundering*, u.å.; Ekobrottsmyndigheten, *Penningtvättsbrott*, u.å.

<sup>22</sup> Ekobrottsmyndigheten, *Penningtvättsbrott*, u.å.

<sup>23</sup> Europol, *Money Laundering*, u.å.

<sup>24</sup> G7-gruppen (Group of Seven) är en informell gruppering som består av sju av världens ledande demokratiska industriländer: G7-länderna är Frankrike, Italien, Japan, Kanada, Storbritannien, Tyskland och USA.

bekämpning av penningtvätt och finansiering av terrorism. FATF:s rekommendationer är omfattande och ställer krav på medlemsländernas rättssystem, då de är av både straffrättslig och administrativ karaktär. En viktig hörnsten i FATF:s system är kriminaliseringen av penningtvättsbrott och finansiering av terrorism samt att ha administrativa regelverk för hur det förebyggande arbetet på området ska gå till. Utifrån rekommendationerna ska medlemsländerna bygga upp hela strukturer med regler och arbetssätt för att bekämpa penningtvätt och finansiering av terrorism.<sup>25</sup>

FATF:s rekommendationer innehåller bland annat riktlinjer gällande kund-due diligence, när finansiella institutioner bör använda dem, vad de bör innehålla och hur länge informationen ska sparas.<sup>26</sup> Rekommendationerna innehåller även ytterligare åtgärder för specifika personer och aktiviteter såsom personer i politiskt utsatt ställning (PEP), banköverföringar, korrespondentbanker, penga- eller värdeöverföringstjänster och ny teknologi.<sup>27</sup>

## 2.3 Europeiska unionens penningtvättsdirektiv

### 2.3.1 EU:s nuvarande penningtvättsdirektiv

Då penningtvätt och finansiering av terrorism ofta bedrivs internationellt har EU valt att beakta internationell samordning och internationellt samarbete i utarbetandet av det fjärde penningtvättsdirektivet eftersom det annars skulle få en mycket begränsad verkan. Åtgärderna som antagits bör därför enligt EU vara förenliga och minst lika stränga som de åtgärder som finns i andra internationella forum. Särskilt fokus läggs på beaktandet av FATF:s rekommendationer och de reviderade FATF-rekommendationerna från 2012.<sup>28</sup>

Fjärde penningtvättsdirektivet är införlivat genom bland annat lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen). I skälen till direktivet anges att penningtvätt är ett hot mot EU:s inre marknad såväl som internationell utveckling då flödet av pengar från kriminell verksamhet kan skada den finansiella sektorns integritet, stabilitet och anseende. Som en del i EU:s arbete med att angripa problemet på unionsnivå infördes direktivet som en del i den straffrättsliga ansatsen genom införandet av förebyggande åtgärder för att motverka att det finansiella systemet utnyttjas för penningtvätt och finansiering av terrorism. EU anser att personer som ägnar sig åt penningtvätt kan försöka utnyttja de friheter som tillhör unionens integrerade finansiella område såsom möjligheten att fritt flytta kapital och tillhandahålla finansiella tjänster.<sup>29</sup> Målsättningen med det fjärde penningtvättsdirektivet var att ytterligare förstärka ramverket för bekämpning av penningtvätt och finansiering av terrorism. Direktivet inkluderar en vidare krets av verksamhetsutövare än tidigare, omfattar i princip de flesta tillhandahållare av

---

<sup>25</sup> Prop. 2016/2017:173 s.170-171.

<sup>26</sup> Financial Action Task Force, *The FATF recommendation*, 2023, s.14-15.

<sup>27</sup> Ibid s.16-17.

<sup>28</sup> Skäl 4, Direktiv 2015/849.

<sup>29</sup> Skäl 1-2, Direktiv 2015/849.

speltjänster, samt omfattar fysiska och juridiska personer som yrkesmässigt handlar med varor i den mån som betalning görs kontant med ett belopp motsvarande 10 000 euro eller mer.<sup>30</sup>

Direktivet slår fast att användningen av en riskbaserad metod är ett effektivt sätt att kartlägga och minska riskerna. Därav finns det krav på att den riskbaserade metoden används. Riskbedömningar ska utföras på tre olika nivåer: Europeiska kommissionen, medlemsstaterna och de individuella verksamhetsutövarna. Direktivet bygger på att verksamhetsutövare har ett ansvar att arbeta förebyggande med att förhindra penningtvätt och de enskilda aktörerna har höga krav på sig. En holistisk riskbaserad metod bör användas för att effektivt kunna hantera de risker som unionen och dess aktörer står inför eftersom riskerna är olika från fall till fall. Åtgärder ska vidtas utifrån en riskbedömning i enlighet med ett antal bestämmelser i direktivet.<sup>31</sup>

Det har även införts ett femte penningtvättsdirektiv (5AMLD) som ett tilläggsdirektiv till fjärde penningtvättsdirektivet. Syftet med direktivet var att förbättra ramverket mot penningtvätt med anledning av den ökade användningen av nya tekniska lösningar och risker gällande virtuella valutor. Direktivet innehåller även ändringar i form av att informationsutbytet mellan olika myndigheter ska effektiviseras samt ett förstärkt skydd för visselblåsare.<sup>32</sup> Direktivet har tagits fram som ett svar på den digitala och tekniska utvecklingen som har förenklat för kriminella att tvätta pengar då de moderna lösningarna inte omfattats av unionsrätten eller varit undantagna. Det har gjort att unionen känt ett behov av att ställa högre krav på kundkännedomsprocessen och riskbedömningen gällande transaktioner och affärsförbindelse från högriskredjeländer och mer okända betalningsverktyg. Unionen vill även skapa mer harmonisering mellan medlemsländerna för en effektivare bekämpning av penningtvätt.<sup>33</sup> Det femte penningtvättsdirektivet utmärker sig på så sätt att när det antogs gick det bortom FATF:s rekommendationer genom att till exempel ställa krav på att medlemsländerna ska reglera tillhandahållare av virtuella valutor. Det är en fråga där FATF tagit efter EU och som numera ingår i deras reviderade rekommendationer.<sup>34</sup>

### 2.3.2 EU:s förslag till nya åtgärder för penningtvätt

I över 30 år har EU arbetat med att bekämpa penningtvätt och finansiering av terrorism. Sedan första direktivet antogs 1991 har det förändrats och ersatts ett flertal gånger. Allt eftersom samhället förändrats har EU:s lagstiftning följt efter för att hantera nya risker som uppstår, såsom digitala valutor, globala terroristorganisationer men även kriminella som exploaterar kryphål i systemet. Detta ledde till att kommissionen 2021 föreslog ett åtgärds paket för att stärka och förbättra EU:s penningtvättsarbete. Åtgärds paketet innehåller ett nytt penningtvättsdirektiv med mekanismer för att förhindra penningtvätt, skapa en ny EU-myndighet som arbetar med Anti-Money Laundering (AML), en förordning om

---

<sup>30</sup> Prop. 2016/17:173 s.171.

<sup>31</sup> Prop. 2016/17:173 s. 178.

<sup>32</sup> Betänkande 2019/20: FiU15: Skärpta åtgärder mot penningtvätt och finansiering av terrorism.

<sup>33</sup> Skäl 2, 9 och 12, Direktiv 2018/843.

<sup>34</sup> M. Forsman, *30 år av penningtvättsbekämpning i Sverige och internationellt – fungerar systemet som det var tänkt?* s.33.

AML-krav för den privata sektorn samt en revision av förordningen om ”transfers of funds”. I början av 2024 enades rådet och parlamentet om ett provisoriskt avtal gällande kommissionens AML-paket.<sup>35</sup> Det som kvarstår är att färdigställa de olika texterna och att dessa formellt ska antas av rådet och parlamentet.<sup>36</sup>

Förordningen har utökat antalet verksamhetsutövare som omfattas av lagstiftningen till att inkludera kryptosektorn. Det gör att verksamhetsutövare som tillhandahåller tjänster kopplade till kryptovaluta behöver utföra due diligence på sina kunder genom att skaffa sig bland annat kundkännedom samt rapportera misstänkt verksamhet. De ska kontrollera kunder som genomför transaktioner med kryptovaluta om värdet överstiger 1000 euro. Även sektorer som handlar med lyxvaror kommer inkluderas i den nya lagstiftningen. Förordningen innefattar även utökade due diligence-åtgärder för gränsöverskridande korrespondentförhållande för verksamhetsutövare som tillhandahåller kryptorelaterade tjänster. Kredit och finansinstitut ska även vidta utökade åtgärder i sina affärsrelationer med väldigt rika individer (high net-worth). Utöver det införs ett högsta tak för kontantköp på 10 000 euro. Verksamhetsutövare måste också identifiera en persons identitet som gör transaktioner mellan 3 000 och 10 000 euro i kontanter. Förordningen skulle även göra reglerna om verklig huvudman mer harmoniserade och transparenta genom att dels ha en tydligare definition av vad verklig huvudman innebär, dels göra det lättare att identifiera vem/vilka som är verklig huvudman. Verksamhetsutövare ska även ha due diligence-åtgärder mot vissa transaktioner som involverar högriskredjeländer som har stora brister i sitt nationella penningtvättsarbete.<sup>37</sup>

I förslaget till direktiv framgår att målet är att förbättra arbetet med att minska risker, effektivt upptäcka kriminellas försök att utnyttja unionens finansiella system för kriminell verksamhet och att stärka den interna marknadens integritet. Förslaget till direktiv syftar till att åtgärda de problem som identifierats med direktiv 2015/849 (fjärde penningtvättsdirektivet) för att skapa tillräcklig motståndskraft och kapacitet i unionens finansiella system för att motverka penningtvätt och terroristfinansiering. En del i det är att underlätta samarbetet mellan unionens medlemsländer.<sup>38</sup>

Det föreslagna direktivet innehåller bestämmelser om att det ska finnas ett register över verkliga huvudmän och att den informationen som lämnas ska verifieras. Den myndighet som har hand om registret har rätt att inspektera de registrerade om det finns tvivel kring informationens riktighet. Dessa register är tillgängliga för myndigheter och verksamhetsutövare men även personer med legitimt intresse, till exempel journalister. Direktivet innehåller även bestämmelser för hur finansiell underrättelsetjänst (FIU) ska motverka, rapportera och bekämpa penningtvätt. Enligt direktivet kommer FIU ha direkt tillgång till finansiell och administrativ information samt information från rättsväsendet. Direktivet lägger precis som tidigare direktiv, fokus på riskbedömning som ett viktigt verktyg och kommer därför att innebära krav på att medlemsstaterna gör en riskbedömning på nationell nivå för att minska de

---

<sup>35</sup> Europarådet, *Fight against money laundering and terrorist financing in the EU*, 2024.

<sup>36</sup> Europarådet, *Anti-money laundering: Council and Parliament strike deal on stricter rules*, 2024.

<sup>37</sup> 2021/0239 (COD); Europarådet, *Anti-money laundering: Council and Parliament strike deal on stricter rules*, 2024.

<sup>38</sup> Skäl 1-3, 2021/0250 (COD).



risker som uppstår.<sup>39</sup> Kommissionen kommer också göra en riskbedömning av medlemsstaterna och lämna rekommendationer.

## 2.4 Nationell lagstiftning gällande penningtvätt

För att införliva det fjärde penningtvättsdirektivet i svensk lagstiftning ersattes den dåvarande penningtvättslagen med samma namn, lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism, med lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism. Det gjordes för att den dåvarande lagen var svår att överblicka i vissa avseende, som en följd av de många ändringar som gjorts vid olika tillfällen. Då det fjärde penningtvättsdirektivet skulle ha inneburit att flera nya paragrafer infördes i lagen hade det kunnat leda till att denna blev än mer svåröverskådlig. Därmed upphävdes den dåvarande penningtvättslagen och ersattes med den nuvarande som trädde i kraft den 1 augusti 2017.<sup>40</sup> Penningtvättslagen ställer krav på och berör ett stort antal aktörer. Dels ställer lagen krav på privata företag i ett antal olika branscher, dels på 16 myndigheter samt Sveriges advokatsamfund, som ska kontrollera att regelverket efterföljs av privata företag och använda sig av informationen som systemet producerar.<sup>41</sup>

Syftet med penningtvättslagen är att förhindra att finansiell och annan näringsverksamhet utnyttjas för penningtvätt och finansiering av terrorism. Verksamhetsutövare ska utforma åtgärder, förfaranden, kontroller m.m. utifrån riskerna för penningtvätt inom den specifika verksamheten och fortlöpande anpassa dessa. Det innebär att flest och mest omfattande åtgärder sätts in där de största riskerna finns och färre och mindre omfattande åtgärder där riskerna är mindre. Genom att verksamhetsutövare använder sig av ett riskbaserat synsätt kan de motverka att deras verksamheter utnyttjas för penningtvätt till en lägre kostnad och högre effektivitet än genom att införa ett detaljreglerat system. Penningtvättslagen är därför utformad så verksamhetsutövaren kan tillämpa det riskbaserade synsättet i hela verksamheten.<sup>42</sup>

## 2.5 Kundkännedom enligt penningtvättslagen

### 2.5.1 Varför behövs kundkännedom?

En grundläggande förutsättning för att en verksamhetsutövare ska kunna försvåra och förhindra att verksamheten utnyttjas för penningtvätt är att de har tillräcklig kunskap om sina kunder, s.k. kundkännedom.<sup>43</sup> Det är i mötet med kund som en verksamhetsutövare har störst möjlighet att upptäcka penningtvätten och motverka riskerna, vilket gör det till det mest handfasta och konkreta redskapet dessa har för

---

<sup>39</sup> 2021/0250 (COD); Europarådet, *Anti-money laundering: Council and Parliament strike deal on stricter rules*, 2024.

<sup>40</sup> Prop. 2016/17:173 s.175.

<sup>41</sup> M. Forsman, s.33.

<sup>42</sup> Prop. 2016/17:173 s.178.

<sup>43</sup> Prop. 2016/17:173 s. 228.

att hantera riskerna.<sup>44</sup> Det är också viktigt för att verksamhetsutövaren ska kunna rapportera misstänkta aktiviteter och transaktioner till Polismyndigheten.<sup>45</sup> Verksamhetsutövare har en skyldighet att granska och rapportera misstänka transaktioner till Finanspolisen (FIPO) utan dröjsmål. Det behöver inte finnas bevis för att penningtvätt faktiskt har skett utan en misstanke räcker.<sup>46</sup>

Kundkännedom uppnås genom att använda företagets allmänna riskbedömning i kombination med den enskilda kundens riskbedömning. Utan tillräcklig kundkännedom får inte företaget etablera eller behålla en affärsrelation, eller utföra enstaka transaktioner (3 kap. 1 § penningtvättslagen). Detsamma gäller om ett företag misstänker att deras produkter och tjänster kan komma att användas för penningtvätt eller finansiering av terrorism. Om ett företag etablerar en affärsrelation med en kund ska de alltid vidta åtgärder för att uppnå kundkännedom, även om det endast skulle gälla en enstaka/några enstaka transaktioner som uppgå till 15 000 euro, eller vid överföring av medel som avses i artikel 3.9 förordning 2015/847<sup>47</sup> om överföringen överstiger ett belopp motsvarande 1 000 euro (3 kap. 4 § penningtvättslagen).<sup>48</sup> Vad som avses med en affärsförbindelse definieras i 1 kap. 8 § 1 som en affärsmässig förbindelse som när den etableras förväntas ha en viss varaktighet. En affärsförbindelse kan uppstå genom konkludent handlande och affärsförbindelsen uppstår inte nödvändigtvis första gången som kund och verksamhetsutövare varit i kontakt med varandra.<sup>49</sup>

Kundkännedom är ett av de verktyg som verksamhetsutövare behöver använda för att upptäcka och motverka penningtvätt. För att få etablera en affärsförbindelse måste en verksamhetsutövare ha tillräcklig kännedom om kunden för att kunna hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen samt övervaka och bedöma kundens aktiviteter och transaktioner enligt 4 kap. 1–2 §§ (3 kap. 1 § penningtvättslagen). Detta gör verksamhetsutövaren genom att inhämta data om den aktuella kunden, vilket används för att förstå syftet med affärsförbindelsen, behandla riskerna samt övervaka kundens transaktioner och aktiviteter.<sup>50</sup> Uppgifter om kunden ska inhämtas löpande och vid behov under en pågående affärsförbindelse för att kunna upptäcka avvikelser med mera.<sup>51</sup>

## 2.5.2 Åtgärder för kundkännedom

I 3 kap. 7–11 §§ penningtvättslagen framgår vilka åtgärder som ska vidtas för identifiering och kontroll av den aktuella kunden. Information som ska samlas in gäller identifiering och kontroll av kundens identitet från en oberoende och tillförlitlig källa (3 kap. 7 § penningtvättslagen). Grundtanken bakom är att inga anonyma transaktioner är tillåtna, men användningen av målvakter och utnyttjade

---

<sup>44</sup> SOU 2016:8, s.199.

<sup>45</sup> Prop. 2016/17:173 s. 228.

<sup>46</sup> Finansinspektionen, *Rapport till FIPO*, 2023.

<sup>47</sup> Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006.

<sup>48</sup> Jfr Finansinspektionen, *Kundkännedom*, 2023.

<sup>49</sup> Prop. 2016/17:173 s.188–189.

<sup>50</sup> Finansinspektionen, *Kundkännedom*, 2023; FATF rekommendationer punkt 10.

<sup>51</sup> Svenska institutet mot penningtvätt, *Grundläggande vägledning om kundkännedom*, 2020 s. 6.

identiteter försvårar identitetskontroller för myndigheter och verksamhetsutövare.<sup>52</sup> I Finansinspektionens föreskrifter framgår det närmare hur kontrollen ska gå till genom att kontrollera en fysik persons ID-handling eller genom att inhämta namn, adress, personnummer eller motsvarande och jämföra handlingarna mot externa register samt skicka bekräftelse till folkbokföringsadressen.<sup>53</sup> Juridisk person kontrolleras genom registreringsbevis eller motsvarande och att kontrollera företrädaren för en juridisk person, varvid det även fastställs om företrädaren har behörighet att företräda den juridiska personen.<sup>54</sup> Till detta har verksamhetsutövaren även en skyldighet att utreda vem som är verklig huvudman då denna utövar ett direkt eller indirekt bestämmande inflytande över kunden och kontrollerar dennes identitet. Verksamhetsutövaren ska utreda kundens ägarförhållande och kontrollstruktur för att kunna göra en riktig riskbedömning. Skulle en juridisk person sakna en verklig huvudman eller den person som identifieras som huvudman inte är den verkliga huvudmannen så ska styrelseordförande, verkställande direktör eller motsvarande anses vara verklig huvudman.<sup>55</sup> Kontroll av kunden och den verkliga huvudmannens identitet ska vara färdig innan en affärsförbindelse får etableras eller en enstaka transaktion utförs (3 kap. 9 § penningtvättslagen).

Är en kund i politisk utsatt ställning (PEP), familjemedlem till någon med PEP, eller känd medarbetare till en sådan person tillkommer skärpta åtgärder för verksamhetsutövaren. Då ska verksamhetsutövaren alltid ta reda på varifrån de tillgångarna kommer som hanteras i en affärsförbindelse eller en enstaka transaktion. Godkännande behöver inhämtas från en behörig beslutsfattare innan en affärsförbindelse får inledas och det ska genomföras fortlöpande uppföljning av affärsförbindelsen.<sup>56</sup> Anledning att PEP pekas ut är att de utgör en högre korruptionsrisk och kan vara mer exponerade för eller iblandade i penningtvättsupplägg.<sup>57</sup> Det gör att banker ska behandla dem som högrisk kunder och tillämpa ökad due diligence.<sup>58</sup> Även beträffande personer som kommer från ett högriskland utanför EES ska verksamhetsutövaren vidta vissa skärpta kundkännedsåtgärder.<sup>59</sup>

En verksamhetsutövare placerar in sina kunder i olika riskplaceringar utifrån deras riskprofil.<sup>60</sup> Kundens riskprofil används tillsammans med övriga omständigheter som utgångspunkt för vilka åtgärder för kontroll, bedömning och utredning som ska göras.<sup>61</sup> Verksamhetsutövaren får tillämpa förenklade åtgärder för kundkännedom om risken för penningtvätt eller finansiering av terrorism som förknippas med kundrelationen anses vara låg. Följaktligen kan kontroller, behandlingar och utredningar vara mer begränsade i sin omfattning och vidtas på ett annat sätt.<sup>62</sup> Enligt Finansinspektionens riktlinjer ska förenklade åtgärder för fysisk och juridisk person

---

<sup>52</sup> M. Forsman s. 35.

<sup>53</sup> Finansinspektionens författningssamling 2017:11 3 kap. 1.2 och 5 §§.

<sup>54</sup> Finansinspektionens författningssamling 2017:11 3 kap. 6–7 §§.

<sup>55</sup> 3 kap. 8 § penningtvättslagen; Finansinspektionen, *Kundkännedom*, 2023; se även FATF rekommendationer punkt 10.

<sup>56</sup> 3 kap. 10 § penningtvättslagen; Finansinspektionen, *Kundkännedom*, 2023.

<sup>57</sup> M. Forsman s.36.

<sup>58</sup> Institutet mot mutor. *PEP- politiskt exponerad person*, u.å.

<sup>59</sup> 3 kap. 11 § penningtvättslagen; Finansinspektionen, *Kundkännedom*, 2023.

<sup>60</sup> 3 kap. 12 § 2.p penningtvättslagen.

<sup>61</sup> 3 kap. 14 § penningtvättslagen.

<sup>62</sup> 3 kap. 15 § penningtvättslagen; Finansinspektionen, *Riskklassificering*, 2023.

begränsas till att verksamhetsutövaren identifierar och kontrollerar den fysiska personens/juridiska personens företrädares identitet genom inhämtning av namn, adress, personnummer eller motsvarande och kontrollera dessa mot externa register med mera. De ska även i begränsad omfattning genomföra övriga åtgärder som anges i 3 kap. 8 och 10–13 §§ penningtvättslagen.<sup>63</sup> Anser verksamhetsutövare däremot att risken med kundrelationen är hög ska särskilt omfattande kontroller göras. De åtgärder som ska göras vid en hög risk kan vara inhämtning av ytterligare information om kundens affärsverksamhet eller ekonomiska situation samt var kundens ekonomiska medel kommer ifrån.<sup>64</sup>

Handlingar och uppgifter som avser åtgärder gällande kundkännedom och transaktioner som kund har genomfört inom ramen för affärsförbindelser eller vid enstaka transaktioner som omfattas av krav på åtgärder för kundkännedom enligt 3 kap. 4–6 §§ ska sparas av en verksamhetsutövare i 5 år efter avslutad affärsförbindelse.<sup>65</sup>

### 2.5.3 Samspelet mellan kundkännedom, riskbedömning och övervakning

Verksamhetsutövare gör en allmän riskbedömning som består av en bedömning av hot och sårbarheter kopplade till verksamhetens kundgrupper, geografisk exponering, produkter och tjänster samt distributionskanaler som kundkännedomsprocessen utgår ifrån. Den allmänna riskbedömningen behövs för att hitta de relevanta riskfaktorerna som verksamheten står inför för att kunna göra en relevant riskbedömning av kunden utifrån de krav som ställs upp av lagstiftningen. Riskbedömningen ligger sedan till grund för den bedömning som görs för att bestämma kundens riskprofil, vilket i sin tur påverkar den löpande uppföljningen och övervakningen. Den allmänna riskbedömningen och de riskfaktorer som verksamhetsutövaren har identifierat styr vilka åtgärder som behöver vitas och deras omfattning, men även omfattningen av processen i övrigt.<sup>66</sup>

Som ett komplement till den kunskap som en verksamhetsutövare har om kunden och dennes affärs- och riskprofil, samt i vissa fall, de ekonomiska medlens ursprung, övervakas även transaktioner (transaktionsövervakning). Genom att kontrollera och dokumentera kundens transaktioner kan verksamhetsutövaren se om den informationen stämmer överens med kunskap som verksamhetsutövaren besitter om kunden. Transaktionsövervakningen är att betrakta som en del av kundkännedomsprocessen och syftar till att se till att handlingar, uppgifter och upplysningar är aktuella. Övervakningen gör att kundens riskprofil anpassas och skulle kunden anses utgöra en hög risk kommer verksamhetsutövaren följa upp kunden mer noggrant än en lågriskkund. Uppföljningen är uppdelad i två delar där den första delen är att fortlöpande analysera kundkännedomen för att kunna göra relevanta bedömningar om den är tillräcklig och om risknivån har förändrats, medan den andra delen är

---

<sup>63</sup> Finansinspektionens författningssamling 2017:11 3 kap. 9–10 §§.

<sup>64</sup> 3 kap. 16 § penningtvättslagen.

<sup>65</sup> 5 kap. 3 § penningtvättslagen.

<sup>66</sup> Svenska institutet mot penningtvätt, *Grundläggande vägledning om kundkännedom*, 2019.

transaktionsövervakning för att se om beteendet från kundens sida är det förväntade eller om det förekommer avvikelser.<sup>67</sup>

---

<sup>67</sup> Finansinspektionen, *Övervakning*, 2023.

## 3 Behandling av personuppgifter vid kundkännedom

### 3.1 Grundläggande om dataskyddsförordningen

#### 3.1.1 Syftet med dataskyddsförordningen

Hur personuppgifter ska hanteras bestäms i 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), mer känd som GDPR.

Det främsta syftet med dataskyddsförordningen är att skydda fysiska personers grundläggande fri- och rättighet särskilt rätten till skydd av personuppgifter. Dataskyddsförordningen gäller således för i princip all behandling av personuppgifter.<sup>68</sup> Rätten till privatliv kommer till uttryck i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR). I artikel 8.1 EKMR ges fysiska personer rätt till respekt för privat- och familjeliv, hem och korrespondens. EU-stadgan om grundläggande rättigheter stadfäster också rätten till respekt för privat- och familjeliv i artikel 7. Genom artikel 8 i EU-stadgan inrättas även en separat rätt till skydd för personuppgifter. I Sverige är det även inskrivet i regeringsformen (RF) att individer har rätt till skydd för den personliga integriteten i samband med behandling av personuppgifter (2 kap. 6 § 2 RF). Samtidigt framgår det av GDPR att rätten till skydd av personuppgifter inte är en absolut rättighet utan att den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.<sup>69</sup> Förordningen syftar även till att säkerställa det fria flödet av personuppgifter inom unionen.<sup>70</sup> Genom att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så kan personuppgifter flöda fritt inom unionen. Det uppnås genom att förordningen är direkt tillämplig i alla medlemsstater och att samma regler gäller inom hela unionen.<sup>71</sup>

#### 3.1.2 Personuppgiftsbegreppet

Personuppgift i dataskyddsförordningens mening är *varje upplysning som avser en identifierad eller identifierbar fysisk person* (även kallad en registrerad).<sup>72</sup> Med varje

---

<sup>68</sup> Artikel 1.2 och art 2 i GDPR.

<sup>69</sup> Skäl 1 och 4 i GDPR.

<sup>70</sup> Artikel 1.3 i GDPR.

<sup>71</sup> IMY, *Syfte och tillämpningsområde*, 2024.

<sup>72</sup> Artikel 4.1 i GDPR.

upplysning avses all information, oberoende av uppgiftens art eller innehåll, om det är objektivt eller subjektivt, riktiga eller oriktiga, känsliga eller okänsliga, privata eller arbets-yrkeslivet. Upplysningarna är även teknikneutrala så de kan vara antingen digitala eller analoga.<sup>73</sup> Med ”som avser” fysisk person menas att uppgiften till sitt innehåll eller genom behandlingens syfte eller resultat är kopplad till en bestämd individ. Det första innebär att uppgiften handlar om en fysisk person. Syfte är att ändamålet med behandlingen är att bedöma, bemöta, särbehandla eller påverka en viss persons uppträdande eller ställning. Resultat är att behandlingen har inverkan på en persons rättigheter eller intressen.<sup>74</sup> Identifierad är när någon har särskilts från andra personer i en grupp och identifierbar är när någon potentiellt kan identifieras antingen direkt eller indirekt.<sup>75</sup> Direkt identifierbar är när den personuppgifts-ansvarige kan identifiera den registrerade genom kompletterande information som denne själv förfogar över och indirekt när personuppgiftsansvarige kan identifiera den registrerade genom kompletterande information som någon annan förfogar över.<sup>76</sup> Med fysisk person avses endast nu levande människor, men den är inte begränsad till medborgare eller invånare i ett visst land.<sup>77</sup> Enligt praxis från EU-domstolen ska personuppgiftsbegreppet tolkas vidsträckt.<sup>78</sup>

### 3.1.3 Materiellt och territoriellt tillämpningsområde

För att GDPR ska vara tillämplig ska behandlingen falla inom tillämpningsområdet. Det innebär att hänsyn ska tas till det materiella, personella, territoriella och det temporala tillämpningsområdet.

Det materiella tillämpningsområdet anger vad som faller under dataskyddsförordningen. Enligt artikel 2 gäller dataskyddsförordningen på helt och delvis automatiserad behandling. Med delvis automatiserad avses till exempel personuppgifter som samlas in manuellt för att sedan sammanställas i dataformat. Även fullständigt manuell behandling kan inkluderas om personuppgifterna ingår i ett register. Vid bedömning om det är ett register eller inte så har det betydelse om informationen är strukturerad så att det lätt går hitta information om en enskild person.<sup>79</sup> Artikel 2 tar även upp när förordningen inte ska tillämpas. Det är fallet i fyra olika situationer: (a) verksamhet som inte omfattas av unionsrätten (b) den gemensamma utrikes- och säkerhetspolitiken, (c) rent privat natur eller hushållet, och (d) behöriga myndigheters brottsbekämpning.

Det territoriella tillämpningsområdet anger var dataskyddsförordningen tillämpas i enlighet med artikel 3. Dataskyddsförordningen tillämpas när personuppgifts-ansvariga eller ett personuppgiftsbiträde har ett verksamhetsställe inom EU och

<sup>73</sup> Artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, WP 136, s. 6–9.

<sup>74</sup> Artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, WP 136, s. 9–12; Domstolens dom av den 20 december 2017, Peter Nowak mot Data Protection Commissioner, C-434/16, ECLI:EU:C:2017:994.

<sup>75</sup> Skäl 26, Dataskyddsförordningen; Domstolens dom av den 19 oktober 2016, Patrick Breyer mot Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779; Artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, WP 136, s.12–22.

<sup>76</sup> Artikel 4.1 i GDPR.

<sup>77</sup> Skäl 2 och 27 i GDPR; Artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, WP 136, s. 22.

<sup>78</sup> EU-domstolens dom, *Novak*, C-434/16, punkt 34.

<sup>79</sup> Domstolens dom av den 10 juli 2018, *Tietosuoja* mot Jehovan todistajat, C-25/17, ECLI:EU:C:2018:551.

behandlar personuppgifter inom ramen för verksamheten oavsett om behandlingen utförs i unionen eller inte. Förordningen gäller även när registrerade befinner sig i unionen men den personuppgiftsansvarige eller ett personuppgiftsbiträde inte är etablerad i unionen, om behandlingen har anknytning till varor och tjänster som utbjudes till registrerade i unionen, även om dessa varor och tjänster skulle vara kostnadsfria, eller om de registrerades beteende övervakas medan de befinner sig i unionen. Förordningen gäller i princip all verksamhet och oavsett vem som utför personuppgiftsbehandlingen. Det kan vara företag, föreningar, organisationer, myndigheter eller privatpersoner.<sup>80</sup>

## 3.2 Rättslig grund för behandling av personuppgifter

### 3.2.1 Rättslig grund

Vid behandling av personuppgifter måste det finnas rättslig grund. Utan rättslig grund är behandlingen av personuppgifter olaglig. Det gäller för både privata och offentliga verksamheter, men grunderna de stödjer sig på är olika. Valet av rättslig grund ska vara dokumenterad och innehålla ett resonemang om varför den rättsliga grunden används. Verksamhetsutövaren ska även informera den registrerade om vilken rättslig grund som används vid behandlingen av personuppgifter, vilket innebär att den rättsliga grunden ska vara fastställd innan behandlingen påbörjas.<sup>81</sup> Integritetskyddsmyndigheten (IMY) gör tolkningen att varje personuppgiftsbehandling ska stödjas på endast en rättslig grund som grundregel och det går inte att byta den rättsliga grunden under pågående behandling.<sup>82</sup>

I samband med Utredningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42) har IMY yttrat sig gällande genomförandet av 2018 års ändringsdirektiv till fjärde penningtvättsdirektivet, gällande vilka rättsliga grunder enligt artikel 6 GDPR, som är starka i arbetet mot penningtvätt. IMY framhåller att rättslig förpliktelse (led c), allmänt intresse (led e) och berättigat intresse (led f) är starka rättsliga grunder som verksamhetsutövare kan stödja sin personuppgiftsbehandling på, vid insamling av kunddata. Samtycke (led a), avtals fullgörande (led b) och skydd av grundläggande intresse (led d) är däremot att betrakta som svaga rättsliga grunder för verksamhetsutövarens behandling av personuppgifter i detta sammanhang.<sup>83</sup>

Vilken rättslig grund som personuppgiftsansvarig valt som stöd för behandlingen påverkar den registrerades möjlighet att invända mot behandlingen. Används rättslig förpliktelse (6.1 led c) som rättslig grund kan den registrerade inte invända mot behandlingen. Skulle däremot behandlingen stödja sig på allmänt eller berättigat intresse (artikel 6.1 led e eller f) har den registrerade rätt att invända mot

---

<sup>80</sup> Artikel 3 i GDPR; IMY, *Syfte och tillämpningsområde*, 2024.

<sup>81</sup> Artikel 6 och skäl 41, 44 och 50 i GDPR; *Rättslig grund*, 2022.

<sup>82</sup> IMY, *Rättslig grund*, 2022.

<sup>83</sup> IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).



behandlingen.<sup>84</sup> I väntan på avgörande i frågan om behandlingen kan grundas på led c eller f kan den registrerade begära begränsning av behandlingen i väntan på kontroll på huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades intressen.<sup>85</sup>

### 3.2.2 Stark rättslig grund

#### 3.2.2.1 Rättslig förpliktelse

Rättslig förpliktelse regleras i artikel 6.1 led c GDPR och används när behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse. Den rättsliga förpliktelsen ska antingen ha grund i EU-rätten eller i nationell lagstiftning och får inte användas som rättslig grund utan stöd i rättsordning. När en bedömning görs av huruvida rättslig förpliktelse följer en lagbestämmelse kan olika förarbetsuttalanden, syftet med bestämmelsen och den rättsliga kontextbestämmelsen behöva beaktas, inte endast ordalydelsen.<sup>86</sup> Enligt Artikel 29-gruppen och IMY kan rättslig förpliktelse användas av finansinstitut för att anmäla vissa misstänkta transaktioner till behöriga myndigheter enligt reglerna om bekämpning av penningtvätt.<sup>87</sup>

#### 3.2.2.2 Allmänt intresse

I artikel 6.1 led e GDPR regleras allmänt intresse. Artikel 6.1 tillåter behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som utgör ett led i den personuppgiftsansvariges myndighetsutövning. Med allmänt intresse avses precis som i led c ett allmänt intresse i EU eller i en medlemsstat. Artikel 6.1 led e är tätt sammankopplat med led c, då det sällan är något som är en rättslig förpliktelse utan att vara av allmän intresse.<sup>88</sup> Däremot kan den registrerade invända mot behandling enligt led e och f enligt artikel 21.1 GDPR något som inte gäller för led c. Artikel 6.1 led e omfattar två olika situationer, dels när en myndighet behandlar personuppgifter som en nödvändig del i sin verksamhet, dels när en icke myndighetsutövande organisation på uppdrag av tredje part som en del i dennes myndighetsutövning, begär att få in uppgifter.<sup>89</sup> IMY anser att behandling som utförs inom ramen för särskilt beslutad samverkan kan ske med stöd i artikel 6.1 led e så länge behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av penningtvättslagen.<sup>90</sup> Det framgår dock av Artikel 29-gruppen att när privata företag lagligt samarbetar med brottsbekämpande myndigheter krävs inte bara en analys enligt artikel 6 utan även att hänsyn tas till principerna om ändamålsbegränsning, lagenlighet och rättvis behandling enligt artikel 5.<sup>91</sup>

---

<sup>84</sup> Artikel 21 i GDPR.

<sup>85</sup> Artikel 18 i GDPR.

<sup>86</sup> S. Öman, 2023.

<sup>87</sup> Artikel 29-arbetsgruppens yttrande 6/2014, s. 20.; IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>88</sup> Artikel 29-arbetsgruppens yttrande 6/2014, s. 22.; S. Öman, 2023.

<sup>89</sup> Artikel 29-arbetsgruppens yttrande 6/2014, s. 22.

<sup>90</sup> IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>91</sup> Artikel 29-arbetsgruppens yttrande 6/2014, s. 23.

### 3.2.2.3 Berättigat intresse (intresseavvägningsregeln)

Berättigat intresse (även kallad intresseavvägningsregeln) återfinns i artikel 6.1 led f och är den sista rättsliga grunden som IMY framhåller som tillräckligt stark för att användas vid motverkandet av penningtvätt. Led f kan användas om behandlingen är nödvändig för den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte registrerades intressen eller dennes grundläggande fri- och rättigheter väger tyngre och kräver skydd av personuppgifter. Myndigheter får dock inte använda sig av led f som rättslig grund när de utför sina uppgifter. Med intresseavvägningsregeln får en personuppgiftsansvarig lämna uppgifterna till tredje part om den har ett berättigat intresse som väger tyngre än den registrerades.<sup>92</sup> Led f fungerar som en sorts säkerhetsventil som öppnar upp för att behandling av personuppgifter som inte faller under 6.1 led a-e kan genomföras. Då bestämmelsen i artikel 6.1 led f GDPR kan jämföras med den tidigare motsvarigheten i dataskyddsdirektivet enligt EU-domstolen finns det tre kumulativa villkor för att behandling av personuppgifter ska vara tillåten. Det första villkoret är att den personuppgiftsansvarige eller tredje part har ett berättigat intresse. För det andra ska behandlingen vara nödvändig för att uppnå det aktuella berättigade intresset. Det sista villkoret är att den registrerades rättigheter inte väger tyngre än det berättigade intresse som behandlingen av personuppgifterna avser att skydda. Frågan om berättigat intresse ska prövas tillsammans med principen om uppgiftsminimering i artikel 5.1 led c.<sup>93</sup> Den avvägning som görs är mycket omfattande och komplex och tar hänsyn till en mängd olika faktorer.<sup>94</sup>

### 3.2.2.4 Avgörande om allmänt och berättigat intresse

I de förenade målen C-37/30 och C-601/20 (*Luxembourg Business Registers*) berörs allmänt och berättigat intresse. EU-domstolen fastslog att bestämmelserna i penningtvättsdirektivet gällande publicering av register på vem som är verklig huvudman var oförenligt med EU-stadgans grundläggande rättigheter. Domstolen klargjorde att det inte var nödvändigt eller proportionerligt att uppgifterna blev tillgängliga för allmänheten även om målet var att motverka penningtvätt. EU-domstolen observerade att verksamhetsutövare kunde visa på berättigat eller legitimt intresse för att få tillgång till offentliga register som innehåller personuppgifter. Domen visar att EU-domstolen anser att delning av individers personuppgifter med tredje part utgör ett allvarligt intrång i de grundläggande rättigheterna.<sup>95</sup>

## 3.2.3 Svag rättslig grund

Samtycke är en svag rättslig grund som i många fall inte är lämplig att stödja sig på utan en alternativ rättslig grund bör i första hand alltid övervägas.<sup>96</sup> Det som gör samtycke till en olämplig rättslig grund är att samtycket ska ges frivilligt, specifikt,

---

<sup>92</sup> Skäl 47 i GDPR.

<sup>93</sup> S. Öman, 2023.

<sup>94</sup> Skäl 47 i GDPR; Artikel 29-arbetsgruppens yttrande 6/2014.

<sup>95</sup> Domstolens dom av den 22 november 2022, *Sovim SA mot Luxembourg Business Registers*, Förenade målen C-37/20 och C-601/20, ECLI:U:C:2022:912.

<sup>96</sup> IMY, *Samtycke*, 2022

informerat och otvetydigt, och kan närsomhelst återkallas.<sup>97</sup> Det innebär att en verksamhetsutövare i sitt arbete mot penningtvätt skulle vara beroende av att kunden skulle ge sitt medgivande till att dennes personuppgifter behandlas samt att denne närsomhelst kan dra tillbaka sitt samtycke. Då en verksamhetsutövare inte får inleda en affärsrelation utan tillräcklig information om kunden utan att bryta mot regler i lagen eller i andra föreskrifter är samtycke inte en säker rättslig grund att använda sig av.<sup>98</sup>

Nästa rättsliga grund att betrakta som svag i bekämpning av penningtvätt är avtalsfullgörande som återfinns i artikel 6.1 led b. Led b används när ”behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås”.<sup>99</sup> Avtalsfullgörandet kan vara ett kundavtal där det är nödvändigt att behandla kunduppgifter men i IMY:s yttrande till Utredningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism anses inte artikel 6.1 led b vara en lämplig rättslig grund vid motverkande av penningtvätt.<sup>100</sup>

Den sista rättsliga grunden är skydd av grundläggande intresse i artikel 6.1 led d. Den gäller behandling av personuppgifter som är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller annan fysisk persons liv och bör endast användas som rättslig grund om ingen annan rättslig grund uppenbart kan användas. Grundläggande intressen kan vara övervakning av humanitära nödsituationer som uppstår vid till exempelvis naturkatastrofer eller epidemier.<sup>101</sup> Då led d är tänkt att användas i nödsituationer är den inte avsedd att användas vid verksamhetsutövares behandling av personuppgifter i arbete med att motverka penningtvätt. Denna rättsliga grund ska endast användas när ingen annan rättslig grund kan användas för personuppgiftsbehandling och samtycke inte kan inhämtas. Verksamhetsutövare som arbetar för att motverka penningtvätt har andra rättsliga grunder att stödja sitt arbete på, vilket gör att skydd av grundläggande intressen till en svag grund för verksamhetsutövare.<sup>102</sup>

### 3.2.4 Lagöverträdelse

I artikel 10 GDPR finns bestämmelser om när ”behandling av personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott” är tillåten.<sup>103</sup> Personuppgifter som rör lagöverträdelse anses inte vara känsliga personuppgifter i den mening som finns enligt dataskyddsförordningen men har ändå ett särskilt skydd enligt artikel 10. Med personuppgifter om lagöverträdelse avses om den registrerade begått ett brott, blivit fälld eller friad i ett brottmål i en domstol, blivit föremål för straffprocessuella tvångsmedel eller misstänkt för konkret brott. Som grundregel får endast myndigheter behandla personuppgifter om lagöverträdelser men det finns undantag för rättsligt anspråk och rättsliga

<sup>97</sup> Artikel 4.11, 6.1 led a och 7.3 i GDPR.

<sup>98</sup> Svenska bankföreningen, *Att bli bankkund*, 2022.

<sup>99</sup> Artikel 6.1 led b i GDPR.

<sup>100</sup> IMY, *Avtal med den registrerade*, 2022; IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>101</sup> Artikel 6.1 led d och skäl 46 i GDPR.

<sup>102</sup> S. Öman, 2023.

<sup>103</sup> Artikel 10 i GDPR.

förpliktelse. Ett exempel på en situation som tillåter annan än myndighet att behandla uppgifter om lagöverträdelse är en bank som misstänker att kund ägnar sig åt penningtvätt och har skyldighet enligt lag att utreda och anmäla penningtvätt. Vill verksamhetsutövare undantas från huvudregeln om att endast myndigheter får behandla personuppgifter ska en ansökan skickas till IMY som tar beslut i frågan.<sup>104</sup>

IMY beviljade tillstånd till Danske Bank 2022 att behandla uppgifter om lagöverträdelse. Danske Bank ansökte om att få hantera uppgifter gällande lagöverträdelse för tidigare kunder hos banken men där banken avslutat kundrelationen på grund av krav enligt penningtvättslagen då banken anmälde kunden till polismyndigheten. Banken fick tillstånd att dela information inom koncernen gällande misstänkt penningtvätt för att den kund som en filial avslutat affärsrelationen med inte skulle kunna vända sig till en annan filial inom koncernen, utan att misstankarna om penningtvätt eller finansiering av terrorism tas i beaktan. IMY framför att banker behöver visa på ett berättigat ändamål i sin ansökan och att kraven som penningtvättslagen ställer på banker är ett sådant ändamål. I fallet med Danske Bank ansåg IMY att bankens intresse vägde tyngre än de registrerades integritetsintresse.<sup>105</sup>

### **3.3 Insamling och lagring av personuppgifter**

#### **3.3.1 Uppgiftsminimering**

Vid behandling av personuppgifter finns det några grundläggande principer som utgör kärnan i dataskyddsförordningen och som sätter de yttersta ramarna för vad som är en tillåten behandling.<sup>106</sup> En av de principerna är uppgiftsminimering som anger att de personuppgifter som samlas in och behandlas ska vara ”adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas”.<sup>107</sup> Personuppgiftsansvarig ska inte behandla fler personuppgifter än vad som är nödvändigt och de personuppgifter som samlas in ska ha en tydlig koppling till ändamålet. En personuppgiftsansvarige får därmed inte samla in personuppgifter för obestämda framtida behov, s.k. ”bra att ha”. En verksamhetsutövare får inte heller samla in mer kunddata som är personuppgiften om kunden än vad som är rättsligt motiverat utifrån den riskbedömning som gjorts enligt reglerna i penningtvättslagen.<sup>108</sup>

#### **3.3.2 Lagringsminimering**

En annan grundläggande princip är principen om lagringsminimering som återfinns i artikel 5.1 led e. Principen innebär att personuppgifter som möjliggör identifiering av registrerad inte får förvaras under en längre tid än vad som är nödvändig för de ändamål som ligger till grund för behandlingen. Personuppgifterna får lagras längre

---

<sup>104</sup> IMY, *Personuppgifter som rör lagöverträdelser*, 2022.

<sup>105</sup> IMY, *Beslut om tillstånd att behandla personuppgifter om lagöverträdelse*, 2022

<sup>106</sup> IMY, *Grundläggande principer*, 2024.

<sup>107</sup> Artikel 5.1 led c i GDPR.

<sup>108</sup> Artikel 6.1 led c och skäl 39 i GDPR; IMY, *Grundläggande principer*, 2024.

om de ska användas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, förutsatt att tillräckliga åtgärder vidtas för att säkerställa den registrerades fri- och rättigheter.<sup>109</sup> När personuppgifterna inte längre behövs ska de antingen raderas eller aidentifieras. Det kan dock finnas vissa handlingar som måste sparas på grund av annan lagstiftning. I penningtvättslagen står det att kunddata, vilket inkluderar vissa personuppgifter, ska sparas till fem år efter avslutad affärsrelation.<sup>110</sup>

### 3.4 Informationsskyldighet gentemot den registrerade

För att det finansiella systemet ska fungera på ett stabilt och effektivt sätt krävs det att samhället och marknaden har förtroende för det.<sup>111</sup> Ett sätt att införliva förtroende för den finansiella sektorn bland kunder är ett starkt konsumentskydd. En del i det konsumentskyddet är att företagen ska göra en bedömning av om kunden förstår produkten eller tjänsten de köper.<sup>112</sup> Det är inte bara gällande finansiella produkter och tjänster som finansiella aktörer har en skyldighet mot sina kunder utan även när kundernas personuppgifter behandlas och om deras personuppgifter varit involverade i en personuppgiftsincident.

Principen om laglighet, korrekthet och öppenhet återfinns i artikel 5.1 led a GDPR. Principen framhåller att personuppgifter ska ha en rättslig grund för behandlingen (laglig), behandlingen ska vara rättvis, skälig, rimligt och proportionerlig i förhållande till den registrerade (korrekt), och det ska framgå klart och tydligt för den registrerade hur personuppgifterna behandlas (öppet).<sup>113</sup> Med behandling omfattas hur personuppgifterna insamlas, används, konsulteras eller på annat sätt behandlas. Enlighet öppenhetsprincipen ska all informationen och kommunikation vara lättillgänglig och lättbegriplig, vilket även innefattar språket som används, under hela behandlingen.<sup>114</sup> Informationen som personuppgiftsansvarige ska delge den registrerade preciseras mer utförligt i artikel 12 GDPR. Några av kraven som ställs på informationen som tillhandahålls den registrerade är att den ska vara kort, koncist, begriplig och i lättillgängligt format.<sup>115</sup> Beroende på om informationen om den registrerade har inhämtats direkt från registrerade eller från tredje part, ska informationen till den registrerade innehålla olika uppgifter. I artikel 13 och 14 GDPR regleras innehållskravet, som innefattar syfte och rättslig grund för behandlingen av personuppgifterna.<sup>116</sup> I 5 kap. 7 § penningtvättslagen föreskrivs dock ett undantag från den registrerades rättigheter enligt artikel 13 och 14 GDPR. Om den registrerades personuppgifter behandlats vid upptäckt av ett avvikande ekonomiskt beteende får personuppgiftsansvarig inte informera den registrerade om detta.<sup>117</sup>

---

<sup>109</sup> Artikel 5.1 led d i GDPR.

<sup>110</sup> Skäl 39 i GDPR; 5 kap. 3 § penningtvättslagen; IMY, *Grundläggande principer*, 2024.

<sup>111</sup> Riksbanken, *Det finansiella systemet*, 2022.

<sup>112</sup> Finansinspektionen, *FI granskar passandebedömningar*, 2024.

<sup>113</sup> IMY, *Grundläggande principer*, 2024.

<sup>114</sup> Skäl 39 i GDPR.

<sup>115</sup> Artikel 29-arbetsgruppens riktlinjer om öppenhet enligt förordning 2016/679, s. 6–7.

<sup>116</sup> Artikel 13–14 i GDPR; Artikel 29-arbetsgruppens riktlinjer om öppenhet enligt förordning 2016/679, s. 7.

<sup>117</sup> 5 kap. 7 § penningtvättslagen.

Den registrerade har rätt att få bekräftelse från den personuppgiftsansvarige på om personuppgifter som rör den registrerade är under behandling, och få tillgång till de uppgifterna genom exempelvis en kopia. Skulle uppgifterna inte stämma har den registrerade rätt att få dessa uppgifter rättade.<sup>118</sup>

En uppmärksam granskning som IMY gjorde mot Klarna Bank gällde informationsskyldigheten (öppenhet) mot kund. Granskningen som IMY gjorde av Klarna gällde huruvida banken hade underrättat sina kunder om personuppgiftsbehandlingen i enlighet med bestämmelserna dataskyddsförordningen. IMY framhöll att Klarna bland annat brustit i att lämna tillräcklig information om ändamålet med behandlingen och vilken rättslig grund de använt sig av vid behandlingen av personuppgifterna. I IMY:s bedömning framgår att informationen som lämnats till kund varit direkt vilseledande. Då Klarna hade överträtt dataskyddsförordningens bestämmelser på flera punkter blev påföljden en administrativ sanktionsavgift på 7,5 miljon kronor.<sup>119</sup>

En annan granskning som IMY gjorde några år senare av Klarna Bank gällde den registrerades rätt till rättelse av felaktiga personuppgifter. I granskningen som IMY gjorde framgick det att en kund hos Klarna begärde rättelse av den e-postadress som var kopplad till ett kreditkort hos banken. Klarna framhöll att de inte hade möjlighet att ändra e-posten då den var knuten till en identifikationspunkt och att kunden skulle behöva beställa ett nytt kort. IMY fann att Klarna bröt mot artikel 12.2 och artikel 16 i dataskyddsförordningen. Artikel 12.2 innebär att en personuppgiftsansvarig ska underlätta den registrerades rätt till rättelse och artikel 16 framhåller den registrerades rätt till rättelse av felaktiga personuppgifter. IMY konstaterade att den lösning som Klarna erbjöd kunden, dvs att få ett nytt kort, har försvårat kundens rätt till rättelse. Då ett bolag inte har rätt att kringgå bestämmelserna i dataskyddsförordningen fann IMY att Klarna bröt mot reglerna i artiklarna 12.2 och 16. Påföljden blev en reprimand i enlighet med artikel 58.2 b då IMY ansåg att det hela var en mindre överträdelse i enlighet med skäl 148 GDPR.<sup>120</sup>

---

<sup>118</sup> Artikel 15–16 i GDPR.

<sup>119</sup> IMY, *Beslut efter tillsyn enligt dataskyddsförordningen- Klarna Bank AB*, 2022.

<sup>120</sup> IMY, *Beslut efter tillsyn enligt dataskyddsförordningen- Klarna Bank AB*, 2024

## 4 Samspelet mellan dataskyddsförordningen och penningtvättslagen

### 4.1 Allmänt om samspelet

Enligt penningtvättslagen har verksamhetsutövaren en skyldighet att samla in kunddata, vilket innefattar personuppgifter om kunden. I 5 kap. penningtvättslagen regleras hur behandlingen av personuppgifter ska gå till. Av 5 kap. 2 § penningtvättslagen framgår det att en verksamhetsutövare får behandla personuppgift för att fullföra sina skyldigheter enligt penningtvättslagen. Ändamålet med lagen är att upptäcka penningtvätt och finansiering av terrorism. Så länge verksamhetsutövaren håller sig till ändamålet kan denne behandla personuppgifter enligt artikel 6.1 led c GDPR då denne har en rättslig förpliktelse enligt lag.<sup>121</sup> Skulle däremot ändamålet med behandlingen förändras behöver verksamhetsutövare dels förhålla sig till principerna i artikel 5 GDPR, dels hitta en ny rättslig grund som är tillämplig enligt artikel 6 GDPR.

I artikel 41 och 43 i fjärde penningtvättsdirektivet framgår att behandlingen av personuppgifter omfattas av det gamla dataskyddsdirektivet.<sup>122</sup> I artikel 41 anges de situationer där personuppgifter får behandlas för att förhindra penningtvätt. Artikel 41.2 anger att personuppgifter endast får behandlas av verksamhetsutövare i syfte att förebygga penningtvätt och finansiering enligt artikel 1 i samma direktiv. Skulle verksamhetsutövare ha en annan avsikt med behandlingen får den inte genomföras med stöd i penningtvättsdirektivet. I artikel 41.3 föreskrivs i likhet med dataskyddsförordningen att verksamhetsutövare ska informera kunden innan affärsförbindelsen eller transaktionen fullbordas att personuppgifterna kommer att behandlas. Det finns dock ett undantag för informationsskyldigheten i artikel 41.4, där det framåt att verksamhetsutövaren kan undgå kravet och begränsa kundens information om den aktuella personuppgiftsbehandlingen för att fullgöra sina skyldigheter enligt regleringen på ett korrekt sätt. Artikel 43 framhåller att behandling av personuppgifter för att förebygga penningtvätt ska beaktas som något som är i det allmännas intresse enligt dataskyddsdirektivet.<sup>123</sup>

Enligt Svenska Bankföreningen uppstår det gränsdragningsproblem mellan dataskydd och penningtvättsarbetet för bankerna. Ett problem som tas upp är principen om lagringsminimering enligt dataskyddsförordningen som innebär att personuppgifterna bara får lagras så länge de behövs för det ändamål de samlats in, annars ska de raderas. Enligt penningtvättslagen ska transaktionshistorik sparas så

---

<sup>121</sup> Artikel 29-arbetsgruppens yttrande 6/2014, s. 20.; IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>122</sup> Jfr med dataskyddsförordningen

<sup>123</sup> Artikel 41 och 43 i fjärde penningtvättsdirektivet.

länge en kund har en affärsförbindelse med banken. Bankföreningen framhåller att vad som ingår i begreppet transaktion är oklart och det finns frågetecken beträffande närliggande information som behövs för att förstå själva transaktionen. Huruvida den närliggande informationen inkluderas i transaktionsbegreppet finns det en viss oklarhet om och bankföreningen framhåller att IMY och Finansinspektionens intressen kan vara motstridiga.<sup>124</sup>

## 4.2 Samverkan i förhållande till bestämmelserna i dataskyddsförordningen

För att motverka penningtvätt är det viktigt att verksamhetsutövare och myndigheter kan samverka genom att utbyta information med varandra i syfte att förebygga, förhindra eller upptäcka penningtvätt. Det samarbetet försvåras genom regler om sekretets och annan tystnadsplikt.<sup>125</sup> Därför infördes ett nytt kapitel i penningtvättslagen om samverkan mot penningtvätt och finansiering av terrorism 2022. Det nya kapitlet innehåller bestämmelser om hur informationsutbyte mellan verksamhetsutövare och myndigheter ska gå till vid misstanke om penningtvättbrott. Innan införandet av nya bestämmelser i penningtvättslagen gjordes i vanligt ordningen en utredning. Den utredningen har fått en del kritik från bland annat IMY.

I IMY:s yttrande framgår att myndighetens främsta fokus ligger på att skydda kundens grundläggande fri- och rättigheter när verksamhetsutövare och myndigheter samverkar genom att dela och behandla personuppgifter. IMY framhåller att reglerna gällande samverkan ger verksamhetsutövare och berörda myndigheter mer genomgripande möjlighet att behandla personuppgifter i syfte att motverka penningtvätt än tidigare. Detta då integritetskänsliga uppgifter som tidigare varit omfattade av sekretets kan lämnas ut till enskilda verksamhetsutövare från myndigheter. Samtidigt konstaterar IMY att dataskyddsförordningen ska efterlevas. Det innebär att en rättslig grund måste finnas för behandlingen enligt artikel 6.1 GDPR.<sup>126</sup>

Utredningen framhåller att rättslig förpliktelse (artikel 6.1 led c) är den rättsliga grund som verksamhetsutövare kan använda sig av vid beslutad samverkan. Däremot är IMY kritisk till om rättslig förpliktelse kan användas som rättslig grund vid beslutad samverkan då det är tveksamt om en rättslig förpliktelse har uppstått i dataskyddsförordningens mening eftersom deltagande i en särskild beslutad samverkan är frivilligt, och därmed har myndighet eller verksamhetsutövare en reell möjlighet att avstå från att lämna ut personuppgifter. IMY är dock öppen för att behandlingen av personuppgifter som sker inom ramen för särskild beslutad samverkan kan göras med stöd av artikel 6.1 led e GDPR så länge behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av penningtvättslagen.<sup>127</sup>

---

<sup>124</sup> Svenska Bankföreningen, *Gränsdragningsproblem mellan dataskydd och penningtvättsarbete*, 2019.

<sup>125</sup> Finansdepartementet, *Samverkan mot penningtvätt och finansiering av terrorism*, 2022.

<sup>126</sup> IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>127</sup> IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).



En annan del som IMY framhåller som viktig gällande samverkan är att integritetskänsliga uppgifter ska ha ett tillräckligt skydd. För att förhindra att uppgifterna som behöriga myndigheter lämna till enskilda verksamhetsutövare lämnas till obehöriga, föreslog utredningen att bestämmelser om tystnadsplikt och särskilt förbehåll ska finnas.<sup>128</sup> Idag återfinns reglerna om tystnadsplikt i 4 a kap. 5 § penningtvättslagen och straffet för att bryta mot tystnadsplikten är böter eller fängelse.<sup>129</sup> I dataskyddsförordningen finns bestämmelser om att personuppgiftsbehandling ska genomföras med en lämplig säkerhetsnivå.<sup>130</sup> Vid avvägning av lämplig säkerhetsnivå ska även riskerna som uppkommer i samband med personuppgiftsbehandlingen enligt artikel 32.2 GDPR beaktas. En lämplig säkerhetsnivå måste även iaktas i sammanband med utbytet av personuppgifter mellan de olika aktörerna. Vid behandling av personuppgifter har den personuppgiftsansvarige en skyldighet att skydda den registrerades rättigheter och skydda den personliga integriteten. Därmed kan krav på bland annat detaljerad dokumentation där en motivering till behandlingen i det enskilda fallet finns. Detta som en del i en öppen och pålitlig behandling av personuppgifter.<sup>131</sup>

### **4.3 Förhållandet mellan dataskyddsförordningen och förslaget till ny penninglagstiftning**

#### **4.3.1 Förordningsförslagets samspel med dataskyddsförordningen**

I förslaget till förordning COM 2021/0239 framgår det att dataskyddsförordningen gäller vid behandling av personuppgifter. Det framgår även att bekämpning av penningtvätt och finansiering av terrorism är av viktigt allmänintresse för alla medlemsländerna.<sup>132</sup> Den registrerade har rätt till sina personuppgifter som behandlas för syftet med förordningen. Undantaget är information som rör en misstänkt transaktion då det skulle undergrävt effektivitet i kampen mot penningtvätt. Den registrerade kan begära att en tillsynsmyndighet kontrollerar lagligheten av behandlingen.<sup>133</sup> Personuppgifter ska behandlas av verksamhetsutövare endast i syfte att förhindra penningtvätt och finansiering av terrorism och får inte vidarebehandlas på ett sätt som är oförenligt med dessa ändamål. Behandling av personuppgifter på grundval av denna förordning för kommersiella ändamål är förbjuden.<sup>134</sup>

Det poängteras att det är viktigt att verksamhetsutövare ser till att personuppgifterna är korrekta, pålitliga och uppdaterade när de utför sitt compliance-arbete.<sup>135</sup> Det framgår också att en konsekvensbedömning (data protection impact assessment), DPIA, bör göras när verksamhetsutövare delar information med varandra. Detta då

---

<sup>128</sup> IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>129</sup> 4 a kap. 5 § penningtvättslagen; 20 kap. 3 § BrB.

<sup>130</sup> Artikel 5.1 led f i GDPR.

<sup>131</sup> IMY:s yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

<sup>132</sup> Skäl 85 i 2021/0239 (COD).

<sup>133</sup> Skäl 90 i 2021/0239 (COD).

<sup>134</sup> Artikel 55 i 2021/0239 (COD).

<sup>135</sup> Skäl 85 i 2021/0239 (COD).

delandet av personuppgifter kan vara av hög risk för fysiska personers fri- och rättigheter.<sup>136</sup>

I artikel 55 framgår att verksamhetsutövare får behandla särskilda kategorier av personuppgifter (artikel 9.1 och artikel 10 GDPR) i den utsträckning det är strikt nödvändigt för att motverka penningtvätt och finansiering av terrorism, förutsatt att vissa skyddsåtgärder vidtas. För artikel 9 finns det krav på att verksamhetsutövare informerar sina kunder eller potentiella kunder om vilka särskilda kategorier av personuppgifter som kan komma att behandlas för att nå upp till de krav som ställs upp i förslaget till ny penningtvättsförordning. De behöver också se till att personuppgifterna är korrekta, uppdaterade och kommer från en säker källa, samt att besluten inte är diskriminerande eller partiska. Utöver det ska skyddsåtgärder genomföras i enlighet med artikel 32 GDPR. För att behandla personuppgifter gällande lagöverträdelse ska verksamhetsutövaren dels följa samma regler som för artikel 9, dels följa några regler som är speciella för artikel 10 GDPR. För att ta del av information enligt artikel 10 GDPR ska uppgifterna ha koppling till penningtvätt på något sätt inklusive förbrott eller finansiering av terrorism. Verksamhetsutövare behöver ha system på plats som skiljer på anklagelser, utredningar, förfaranden och fällande domar, med beaktande av den grundläggande rätten till en rättvis rättegång, rätten till försvar och oskuldspresumtionen.<sup>137</sup>

#### **4.3.2 Direktivförslagets samspel med dataskyddsförordningen**

I förslaget till direktiv framgår att dataskyddsförordningen gäller vid behandling av personuppgifter för ändamålet med direktivet. Direktivet framhäver att bekämpandet av penningtvätt och finansiering av terrorism är av vikt för unions medlemsländer men att samtidigt ska verksamhetsutövare och myndigheter respektera regleringen kring behandling av personuppgifter.<sup>138</sup> Det framgår även att den registrerade har rätt att få tillgång till de personuppgifter som behandlas på grund av direktivet. Dock har den registrerade inte rätt till information som handlar om misstänkt rapporterad aktivitet då det skulle få en negativ inverkan på arbetet med att motverka penningtvätt. Direktivet framhäver att i sådant fall kan artikel 23 och artikel 25 GDPR användas för att hindra den registrerade att ta del av informationen. Den registrerade har däremot rätt att be europeiska datatillsynsmannen (EDPS) att kontrollera om behandlingen är laglig enligt artikel 51 och artikel 79 GDPR.<sup>139</sup>

Fysiska personer ska informeras om dataskyddslagstiftningen när deras personuppgifter behandlas i nationella register, såsom registret över verkliga huvudman. Utöver det framgår att endast personuppgifter som är uppdaterade och aktuella (artikel 5.1 led d GDPR) gällande den verkliga huvudmannen får vara tillgängliga samt att den verkliga huvudmannen ska ha informerats om dennes rättigheter enligt dataskyddsförordningen och hur dessa rättigheter kan användas i praktiken. Den verkliga huvudmannen har även rätt att få vetskap om vilka som tagit del av personuppgifterna i enlighet med artikel 15.1 led c GDPR. Där det står att den registrerade har rätt till bekräftelser på huruvida dennes personuppgifter håller på att

---

<sup>136</sup> Skäl 84b i 2021/0239 (COD).

<sup>137</sup> Artikel 55 och skäl 86a i 2021/0239 (COD).

<sup>138</sup> Skäl 85 i 2021/0250 (COD).

<sup>139</sup> Skäl 87 i 2021/0250 (COD).

behandlas. Den registrerade behöver alltså själv begära att ta del av uppgifterna. För att det ska fungera ska den myndighet som har hand om registret över verklig huvudman även ha uppgifter om vem som tagit del av informationen.<sup>140</sup>

Det framgår även av artikel 53 att det är tillåtet att behandla särskilda kategorier av personuppgift (artikel 9.1 GDPR) och personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott (artikel 10 GDPR), om det är strikt nödvändigt och tillräckliga skyddsåtgärder vidtas för att skydda den registrerades rättigheter och friheter. Det finns krav på skyddsåtgärder såsom att endast vissa speciellt utsedda personer få behandla särskilda kategorier av personuppgifter och att det ska göras en bedömning från fall till fall om det är en nödvändig behandling. Personen som behandlar uppgifterna ska vara kompetent och behandla uppgifterna med sekretess och integritet. Det finns även krav på att tekniska och organisatoriska åtgärder vidtas för att säkerställa lämplig säkerhet för personuppgifterna. Dessa åtgärder gäller vid behandling av personuppgifter i både artikel 9.1 och artikel 10 GDPR.<sup>141</sup>

---

<sup>140</sup> Artikel 12.5 och skäl 38 i 2021/0250 (COD).

<sup>141</sup> Artikel 53.1 i 2021/0250 (COD); jfr art 5.1 led f Dataskyddsförordningen.

## 5 Avslutande diskussion

Den digitala utvecklingen gynnar inte bara den ekonomiska tillväxten utan också den ekonomiska brottligheten. Den nya tekniken har öppnat upp för nya tillvägagångsätt för kriminella att tvätta pengar genom kryphål i det finansiella systemet. Det är inte bara ett problem i Sverige, utan ett globalt problem. Därför har länder gått samman för att tillsammans ta krafttag och bekämpa penningtvätt och finansiering av terrorism. Det sker både internationellt genom till exempel FATF:s rekommendationer, men även genom EU-regleringar och nationell lagstiftningen.

I enlighet med lagstiftningen åläggs verksamhetsutövare ett antal förpliktelser gällande insamling och behandling av personuppgifter i sitt arbete med att motverka penningtvätt. Verksamhetsutövare har en förpliktelse att inhämta uppgifter om sina kunder för att skapa och upprätthålla kundkännedom enligt bestämmelserna i penningtvättslagen. God kundkännedom är en central del i verksamhetsutövares arbete med att motverka penningtvätt och är en förutsättning för att det ska få finnas en affärsrelation mellan verksamhetsutövare och kund. Eftersom förutsättningarna för en affärsrelation kan förändras är det viktigt att uppdatera kundkännedomen och följa upp den med jämna mellanrum. Dock finns det inga bestämmelser för hur frekvent det ska göras men minst var femte år är det vanliga.

Kundkännedomsprocessen innebär att både kundens personliga och ekonomiska information behandlas för att verifiera och identifiera dennes identitet. Det görs för att kunna placera in kunden i rätt risknivå. Risknivån avgör vilka åtgärder som behöver vidtas från verksamhetsutövares sida, ju högre risknivå, ju fler åtgärder behövs. En kategori med kunder som klassificeras som högrisk är PEP och deras familj. Är en kund PEP vidtas extra åtgärder då de anses vara högre korruptionsrisk och vara mer exponerade för eller iblandade i penningtvättsupplägg. Det går att diskutera om det faktiskt är nödvändigt utifrån att det innebär intrång i den personliga integriteten inte bara för den med PEP men också dennes familj och andra närstående. Det är dock tillåtet enligt både penningtvättslagen och dataskyddsförordningen att behandla personuppgifter av känslig karaktär om de är nödvändigt för att uppnå penningtvättslagens bestämmelser. Behöver en verksamhetsutövare göra en mer ingående riskbedömning får mer omfattande information inhämtas för att avgöra kundens risknivå.

Det finns dock ett problem. Exakt vad som menas med god kundkännedom framgår varken av lag eller praxis. En verksamhetsutövare ska inhämta information om affärsförbindelsens syfte och art som kommer ligga till grund för en bedömning för vilka aktiviteter och transaktioner som kan förväntas av kunden och för att riskklassificera kunden. Vad som anses som tillfredställande kundkännedom utifrån de kriterierna är dock vagt. Det kan å ena sidan vara att få in tillräckligt tillfredsställda svar av kunden som inte anses behöva fler följdfrågor, till å andra sidan kräva mer detaljerade svar av kunden på avsikten med transaktionerna.

En sak som däremot är tydlig är att verksamhetsutövare måste följa dataskyddsförordningen när de behandlar personuppgifter för att få kundkänedom. De behöver bland annat beakta principerna i artikel 5 GDPR och ha en rättslig grund att stödja sin behandling på enligt artikel 6 GDPR. IMY har yttrat sig om att de rättsliga grunder som en verksamhetsutövare kan grunda sitt penningtvättsarbete på är rättslig förpliktelse, allmänt och berättigat intresse. Av dem är rättslig förpliktelse den strakaste då kunden inte har möjlighet att invända mot behandlingen på det sätt som kunden har vid allmänt och berättigat intresse. Då kunden inte har några möjligheter att invända mot behandlingen vid rättslig förpliktelse kan det finnas en större risk för integritetskränkning. Att motsätta sig behandlingen kan även leda till att relationen avslutas. Det har dock visat sig genom IMY:s två granskningar av Klarna att verksamhetsutövare inte kan göra hur som helst utan de måste följa dataskyddsförordningen när de behandlar personuppgifter.

Allmänt- och berättigat intresse anser IMY också är lämpliga grunder för att motverka penningtvätt. Speciellt när det gäller samverkan där rättslig förpliktelse inte anses vara en lämplig rättslig grund kan enligt IMY allmänt- och berättigat intresse i stället vara aktuellt. Skillnaden mot rättslig förpliktelse är att vid allmänt intresse har kunden möjlighet att göra invändningar mot behandlingen och vid berättigat intresse ska en avvägning göras där kundens fri- och rättigheter ska vägas mot verksamhetsutövarens intressen. Från tidigare uttalanden från IMY framgår det att kundens integritetsintresse kan överväga i enskilda fall men det har också funnits fall där verksamhetsutövarens intresse anses väga tyngre. Frågan är huruvida de flesta kunder faktiskt har vetskap om sina rättigheter enligt dataskyddsförordningen eller möjlighet att förstå dem. Det finns en risk att verksamhetsutövare utnyttjar sin ställning samt att deras kunder sätter stor tilltro till dem. Det finns även en risk för att verksamhetsutövare, såsom banker eller försäkringsbolag, som har en betydande roll för att fysiska personers liv ska fungera smidigt i vardagen, att det kan leda till att kunderna inte vågar ifrågasätta till exempel behandlingen av deras personuppgifter då dessa behövs för att få ha kvar en affärsrelation.

Utifrån vad som framgår av penningtvättsdirektivet och penningtvättslagen så överensstämmer dessa med dataskyddsförordningen. Det är delvis den uppfattningen som framgår av uppsatsen men en avsaknad av vägledande tolkning på området skapar frågetecken. Det är svårt att dra en slutsats om bristen på rättsfall är positivt eller negativt för kunden men den hade varit av värde för verksamhetsutövare. Det hade kunnat bidra med tydligare riktlinjer kring hur dessa ska agera gällande att ta sitt ansvar enligt penningtvättslagen men samtligt minimera risken för integritetsintrång. Av vad som framgår har penningtvättslagen en tendens att göra intrång i fysiska personers privatliv och vara integritetskränkande. Huruvida den faktiskt tar hänsyn till de grundläggande fri- och rättigheterna i enskilda fall kan diskuteras. IMY påpekar att det finns förbättringsåtgärder för att skydda individens fri- och rättigheter, och att det är viktigt att göra det. Samtidigt anser EU att arbetet med att motverka penningtvätt är av stor vikt, vilket gör att det framstår som att verksamhetsutövares berättigade intresse och det allmänna intresset står över individens rättigheter och friheter i frågor som rör penningtvättslagstiftningen.

Genom förslagen till nytt penningtvättsdirektiv och penningtvättsförordning kommer nuvarande lagstiftning att ersättas. Den nya lagstiftningen är i mångt och

mycket ganska lik den nuvarande men inkluderar även en del nya regler om kryptovalutor, verklig huvudman och utökad due diligence. Förslaget tar större hänsyn till individens rättigheter och friheter än vad nuvarande lagstiftning gör. Genom att uttrycka att den personliga integriteten ska respekteras vid penningtvättsåtgärder samt sätta krav på hur särskilda kategorier av personuppgifter ska behandlas visar EU att unionen tycker det är viktigt att följa dataskyddsförordningen och respektera individens rättigheter och friheter. Däremot finns det frågetecken även kring förslaget till direktiv gällande register över verkliga huvudmän. Där framgår att personer med legitimt intresse ska kunna få tillgång till registret och att även om den verkliga huvudmannen kan få veta vem kan denne inte motsätta sig behandlingen. Det går emot mål C-37/20 och C-601/20 *Luxembourg Business Registers* där det framgick att publiceringen av register av verklig huvudman var oförenligt med EU-stadgan. Skillnaden är dock att det tidigare registret var publikt och enligt förslaget ska någon ha legitimt intresse för att få tillgång. Det verkar dock inte vara speciellt höga krav på vad som anses vara legitimt intresse. Hur det blir i verkligheten är svårt att förutse och en ny framtida praxis kan behövas.

Avslutningsvis kan slutsatsen dras att dataskyddsförordningen påverkar verksamhetsutövare i deras kundkännedomprocess genom att ställa krav på att de följer principerna i artikel 5.1 GDPR samt har en rättlig grund att basera sin behandling på. Även om reglerna kan anses som någorlunda enhetliga med varandra finns det förhoppningar om att de nya reglerna ska förtydliga förhållandet mellan penninglagstiftningen och dataskyddsförordningen, samt ge svar på hur den personliga integriteten ska skyddas. Det finns därmed ständigt förbättringsmöjligheter för att skydda individens rättigheter och friheter. I dagsläget läses penningtvättsdirektivet i ljuset av EU:s dataskydds rätt, med hänsyn till ökad öppenhet och skydd för personlig integritet.

# Källförteckning

## Offentligt tryck

Europeiska unionen

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

Proposal for a directive of the European parliament and of the council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM 2021/0250

Proposal for a regulation of the European parliament and of the council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM 2021/0239

### *Artikel 29-gruppen*

Artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, WP 136

Artikel 29-arbetsgruppens yttrande 6/2014 om begreppet den registeransvariges berättigande intressen i artikel 7 i direktiv 95/46/EG. 844/14/EN, WP 217.

Artikel 29-arbetsgruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679. 17/SV, WP260.

Sverige

### *Statens offentliga utredningar*

SOU 2016:8 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism – fjärde penningtvättsdirektivet – samordning – nya penningtvättslag

SOU 2021:42 Stärkta åtgärder mot penningtvätt och finansiering av terrorism

### *Propositioner*

Prop. 2016/17:173 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism

Prop. 2021/22:251 Samverkan mot penningtvätt och finansiering av terrorism

## Rapporter och övriga publikationer

Betänkande 2019/20: FiU15. Finansutskottet. *Skärpta åtgärder mot penningtvätt och finansiering av terrorism.*

Ekobrottsmyndigheten. 2021. *Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020–2021.*

Finansinspektionen. Finansinspektionens författningssamling. 2017. *Finansinspektionens föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism.*

Lagrådsremiss: Finansdepartementet. 2022. *Samverkan mot penningtvätt och finansiering av terrorism.*

Remissvar: Integritetsskyddsmyndigheten (IMY). 2021. *Yttrande över betänkandet Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).*  
Diarienummer: DI-2021-5157

## Litteratur

Bernitz, Ulf, m.fl. *Finna rätt. Juristens källmaterial och arbetsmetoder.* 16 uppl. Stockholm: Nordstedts Juridik AB, 2023.

FATF. 2023. *The FATF recommendations* (FATF: s rekommendationer).

Finansinspektionen. 2019. *FI:s arbete mot penningtvätt och finansiering av terrorism.*

Forsman, Markus. 2020. *30 år av penningtvättsbekämpning i Sverige och internationellt – fungerar systemet som det var tänkt?.* Sveriges Riksbank.

Nääv, Maria & Zamboin, Mauro (red.) *Juridisk metodlära.* 2:3. Uppl. Lund: Studentlitteratur, 2021.

Svenska institutet mot penningtvätt. 2020. *Grundläggande vägledning om behandling av personuppgifter.* 2 uppl.

Öman, Sören. *Dataskyddsförordningen (GDPR) m.m.: en kommentar.* 2.B uppl. Nordstedts Juridik AB, 2023. (E-bok).



## Rättsfall och myndighetsbeslut

Europeiska unionens domstol

Domstolens dom av den 22 november 2022, Sovim SA mot Luxemburg Business Registers, Förenade målen C-37/20 och C-601/20, ECLI:U:C:2022:912.

Domstolens dom av den 19 oktober 2016, Patrick Breyer mot Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779.

Domstolens dom av den 20 december 2017, Peter Nowak mot Data Protection Commissioner, C-434/16, ECLI:EU:C:2017:994.

Domstolens dom av den 10 juli 2018, Tietosuojavaltuutettu mot Jehovan todistajat, C-25/17, ECLI:EU:C:2018:551.

### Myndighetsbeslut

Integritetskyddsmyndigheten (IMY). 2022. *Beslut efter tillsyn enligt dataskyddsförordningen – Klarna Bank AB*. Diarienummer: DI-2019-4062.

Integritetskyddsmyndigheten (IMY). 2024. *Beslut efter tillsyn enligt dataskyddsförordningen – Klarna Bank AB*. Diarienummer: IMY-2023-8336

Integritetskyddsmyndigheten (IMY). 2022. *Beslut om tillstånd att behandla personuppgifter om lagöverträdelse*. Diarienummer: DI-2021-2183.

### Internetkällor

Ekobrottsmyndigheten. 2021. *EBM:s lägesbild om ekonomisk brottslighet i Sverige*.

Tillgänglig online: <https://www.ekobrottsmyndigheten.se/lagesbild/>  
[Hämtad 2024-03-25]

Ekobrottsmyndighet, U.å. *Penningtvättsbrott*.

Tillgänglig online: <https://www.ekobrottsmyndigheten.se/om-ekobrott/brotten-vi-utreder/penningtvattsbrott/>  
[Hämtad 2024-03-25]

Europarådet. 2024. *Fight against money laundering and terrorist financing in the EU*.

Tillgänglig online: <https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/>  
[Hämtad 2024-05-04]

Europarådet. 2024 *Anti-money laundering: Council and Parliament strike deal on stricter rules*.

Tillgänglig online:

<https://www.consilium.europa.eu/en/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-strict-rules/>  
[Hämtad 2024-05-04]

Europol. U.å. *Money Laundering*.  
Tillgänglig online: <https://www.europol.europa.eu/crime-areas/economic-crime/money-laundering>  
[Hämtad 2024-03-25]

Finansinspektionen. 2024. *FI granskar digitala passandebedomningar*.  
Tillgänglig online: <https://www.fi.se/sv/publicerat/nyheter/2024/fi-granskar-digitala-passandebedomningar/>  
[Hämtad 2024-04-25]

Finansinspektionen. 2023. *Kundkännedom*.  
Tillgänglig online: <https://www.fi.se/sv/bank/penningtvatt/process/kundkannedom/>  
[Hämtad 2024-03-25]

Finansinspektionen. 2023. *Rapport till FIPO*. Tillgänglig online:  
<https://www.fi.se/sv/bank/penningtvatt/process/rapport-till-fipo/>  
[Hämtad 2024-04-10]

Finansinspektionen. 2024. *Riskbedömning*.  
Tillgänglig online: <https://www.fi.se/penningtvatt-riskbedomning#fk>  
[Hämtad 2024-03-25]

Finansinspektionen. 2023. *Penningtvätt*.  
Tillgänglig online: <https://www.fi.se/sv/bank/penningtvatt/>  
[Hämtad 2024-03-25]

Institutet mot mutor. U.å. *PEP-politiskt exponerad person*.  
Tillgänglig online: <https://www.institutetmotmutor.se/kunskapsbank/ordlista/pep-politiskt-exponerad-person/>  
[Hämtad 2024-04-12]

Integritetsskyddsmyndigheten. 2024. *Grundläggande principer*.  
Tillgänglig online: <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/>  
[Hämtad 2024-04-22]

Integritetsskyddsmyndigheten. 2022. *Personuppgifter som rör lagöverträdelser*.  
Tillgänglig online: <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgifter-som-ror-lagovertradelser/>  
[Hämtad 2024-04-20]

Integritetsskyddsmyndigheten. 2022. *Samtycke*.  
Tillgänglig online: <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/>  
[Hämtad 2024-04-19]

Integritetsskyddsmyndigheten. 2022. *Rättslig grund*.  
Tillgänglig online: <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/>  
[Hämtad 2024-04-19]

Riksbanken. 2022. Det finansiella systemet.  
Tillgänglig online: <https://www.riksbank.se/sv/finansiell-stabilitet/det-finansiella-systemet/>  
[Hämtad 2024-04-25]

Sas institute. U.å. *Penningtvätt: Vad är AML och varför är det viktigt*,  
Tillgänglig online: [https://www.sas.com/sv\\_se/insights/fraud/anti-money-laundering.html](https://www.sas.com/sv_se/insights/fraud/anti-money-laundering.html)  
[Hämtad 2024-03-25]

Svenska Bankföreningen. 2022. *Att bli bankkund*.  
Tillgänglig online: <https://www.swedishbankers.se/foer-bankkunder/att-bli-bankkund/att-bli-bankkund/>  
[Hämtad 2024-04-22]

Svenska Bankföreningen. 2019. *Gränsdragningsproblem mellan dataskydd och penningtvättsarbete*.  
Tillgänglig online:  
<https://www.swedishbankers.se/repository/bankfokus/bankfokus-nr-2-2019/graensdragningsproblem-mellan-dataskydd-och-penningtvaettsarbete/>  
[Hämtad 2024-05-04]