LUNDS UNIVERSITET
EKONOMI-
HÖGSKOLAN

Rätten till integritet vid bekämpning av penningtvätt

En undersökning av motstridiga krav mellan AML-regleringen och dataskyddsförordningen

Sara Andersson

Affärsjuridisk kandidatuppsats

(HARH13)

15 högskolepoäng

HT 2025

Sammanfattning

Bekämpningen av penningtvätt utgör ett centralt samhällsintresse inom Europeiska unionen och har gett upphov till ett omfattande regelverk som ställer långtgående krav på att verksamhetsutövare behandlar och lagrar personuppgifter. Samtidigt har skyddet för den personliga integriteten stärkts genom EU:s allmänna dataskyddsförordning (GDPR). Regelverken är inte direkt motstridiga, men förutsätter en löpande rättslig avvägning eftersom de ska tillämpas parallellt på samma personuppgiftsbehandlingar.

Frågan aktualiseras särskilt inom digitala finansiella tjänster, där kreditinstitut, betalningsinstitut och andra aktörer genomför automatiserade kundkännedoms- och övervakningsåtgärder i stor skala. Syftet med uppsatsen är att analysera hur kraven på personuppgiftsbehandling enligt penningtvättsregelverket (Anti-Money Laundering, AML) ska tillämpas i förhållande till GDPR:s skydd för den personliga integriteten. Fokus ligger på bevarande av kundkännedomsuppgifter och begränsningar av informationsskyldigheten vid rapportering av misstänkta transaktioner. Analysen utgår från EU-rätten och svensk rätt samt prövar dessa åtgärder mot EU:s stadga om de grundläggande rättigheterna. Uppsatsen använder en rättsdogmatisk metod.

Resultatet visar att penningtvättsregelverket i grunden innebär legitima inskränkningar av den personliga integriteten som motiveras av ett betydande allmänintresse. Samtidigt framkommer att generella lagringstider och omfattande sekretessundantag riskerar att gå längre än vad som är nödvändigt i enskilda fall, särskilt i förhållande till lågriskkunder. Detta aktualiserar behovet av en mer nyanserad tilllämpning där effektiv brottsbekämpning förenas med ett reellt dataskydd.

Ämnesord: penningtvätt, AML, GDPR, dataskydd, öppenhetsprincipen, fintech, kundkännedom, informationsskyldighet.

Abstract

The fight against money laundering constitutes a central public interest within the European Union and has resulted in an extensive regulatory framework imposing far-reaching obligations on obliged entities to process and retain personal data. At the same time, the protection of personal privacy has been strengthened through the EU General Data Protection Regulation (GDPR). Although these regulatory frameworks are not inherently contradictory, their parallel application to the same personal data processing requires an ongoing legal balancing. The issue is particularly evident in digital financial services, where credit institutions, payment institutions, and other actors carry out large-scale automated customer due diligence and monitoring measures.

The purpose of this thesis is to analyse how the requirements for personal data processing under the anti-money laundering (AML) framework should be applied in relation to the privacy protections established by the GDPR. The analysis focuses on the retention of customer due diligence data and limitations to the duty to provide information when reporting suspicious transactions. The study is based on EU law and Swedish law and evaluates these measures in light of the EU Charter of Fundamental Rights. A legal dogmatic method is applied.

The findings show that the AML framework, in principle, entails legitimate restrictions on personal privacy justified by a significant public interest. However, the analysis also demonstrates that general retention periods and broad confidentiality exceptions risk exceeding what is necessary in individual cases, particularly with regard to low-risk customers. This highlights the need for a more nuanced application in which effective crime prevention is balanced with meaningful data protection.

Keywords: Anti-Money Laundering, GDPR, data protection, the principle of proportionality, fintech, Customer Due Diligence.

Innehåll

Förkortningar

AML	Anti-Money Laundering (åtgärder mot penningtvätt)
AMLD	Anti-Money Laundering Directive (EU:s penningtvättsdirektiv)
AMLR	Anti-Money Laundering Regulation (EU:s förordning om penningtvätt)
AMLA	Anti-Money Laundering Authority (EU:s tillsynsmyndighet mot penningtvätt)
EDPB	European Data protection Board (Europeiska dataskyddsstyrelsen)
EU	Europeiska unionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
FATF	Financial Action Task Force
FFFS	Finansinspektionens författningssamling
FI	Finansinspektionen
GDPR	General Data Protection Regulation (EU:s dataskyddsförordning)
KYC	Know Your Customer (kundkännedom)
LED	Law Enforcement Directive (brottsdatadirektivet)
PEP	Politically Exposed Person (person i politiskt utsatt ställning)
SAR	Suspicious Transaction Report
SFS	Svensk författningssamling
SOU	Statens offentliga utredningar
UBO	Ultimate Beneficial Owner (verklig huvudman)

1 Inledning

1.1 Bakgrund

Bekämpningen av penningtvätt (Anti-Money Laundering, AML) och finansiering av terrorism har under de senaste decennierna successivt stärkts inom unionsrätten och kommit att utgöra ett centralt inslag i EU:s finansiella och brottsförebyggande regelverk.[1]I takt med ökad globalisering, digitalisering och gränsöverskridande finansiella flöden har den ekonomiska brottsligheten blivit alltmer komplex och svårupptäckt. Mot denna bakgrund fungerar penningtvätt inte som en isolerad företeelse, utan som ett möjliggörande led för annan allvarlig brottslighet såsom narkotikahandel, bedrägerier, skattebrott och organiserad brottslighet. Den svenska penningtvättslagen syftar därför till att förhindra att det finansiella systemet utnyttjas för att omsätta vinster från brottslig verksamhet och utgör enligt förarbetena en central del i arbetet med att upprätthålla det finansiella systemets integritet.[2] Inom detta preventiva system har banker och andra verksamhetsutövare tilldelats en central kontrollfunktion genom skyldigheter att identifiera kunder, övervaka transaktioner och rapportera misstänkta förhållanden.

Frågorna aktualiseras särskilt inom den framväxande fintech-sektorn, det vill säga företag som tillhandahåller finansiella tjänster genom digitala plattformar, exempelvis betalningsinstitut, e-pengaföretag och digitala kreditgivare. Verksamheten kännetecknas av automatiserade kundprocesser, kontinuerlig transaktionsanalys och behandling av stora datamängder i realtid.[3] Dessa aktörer omfattas av samma penningtvättsrättsliga skyldigheter som traditionella finansiella institut, men fullgör dem ofta genom teknikbaserade lösningar där personuppgiftsbehandlingen utgör en integrerad del av tjänsten.

---

[1] Europeiska kommissionen, Förslag till Europaparlamentets och rådets förordning om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, 20.7.2021, COM(2021) 420 final.

[2] Prop. 2016/17:173, ”En effektivare bekämpning av penningtvätt”, 2017, s. 1 f.

[3] Financial Stability Board (FSB), *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits*, 2017, s. 3.

Det penningtvättsrättsliga regelverket (AML-regelverket) bygger i stor utsträckning på att verksamhetsutövaren samlar in, analyserar och bevarar personuppgifter i syfte att identifiera avvikande beteenden och misstänkta transaktioner. Kundkännedomsåtgärder, löpande övervakning och rapporteringsskyldighet till myndigheter utgör kärnan i detta system. Åtgärderna innebär samtidigt betydande ingrepp i den personliga integriteten, bland annat genom kontinuerlig övervakning och begränsningar i den registrerades möjlighet att få information om behandlingen.

Parallellt har skyddet för personuppgifter harmoniserats genom EU:s dataskyddsförordning (GDPR), som syftar till att säkerställa en hög nivå av skydd för fysiska personers grundläggande rättigheter enligt artiklarna 7 och 8 i EU:s stadga om grundläggande rättigheter (EU-stadgan). Förordningen bygger på principer om bland annat öppenhet, ändamålsbegränsning och lagringsminimering samt ger bland annat den registrerade rätt till information och i vissa fall radering av uppgifter. Rättigheterna är dock inte absoluta utan kan begränsas när det är nödvändigt för att tillgodose legitima samhällsintressen.

Penningtvättsregelverket och dataskyddsregelverket är således avsedda att tillämpas parallellt på samma personuppgiftsbehandlingar. Detta kan ge upphov till en målkonflikt, vilket innebär att det i praktiken krävs en avvägning. Särskilt uppkommer tolkningsfrågor beträffande dels hur länge kundkännedomsuppgifter får bevaras, dels i vilken utsträckning informationsskyldigheten kan begränsas vid övervakning och rapportering av misstänkta transaktioner.

EU-rätten tillhandahåller ett ramverk för denna avvägning. Artikel 23 GDPR möjliggör begränsningar av vissa registrerades rättigheter, medan artikel 52.1 i EU-stadgan uppställer krav på lagstöd, nödvändighet och proportionalitet vid inskränkningar av grundläggande rättigheter. Den rättsliga frågan blir därmed hur de intrång i den personliga integriteten som penningtvättsåtgärder innebär ska bedömas när regelverken tillämpas samtidigt.

1.2 Syfte och frågeställningar

Syftet med uppsatsen är att beskriva och analysera hur penningtvättsregelverkets krav på behandling av personuppgifter ska tillämpas i förhållande till dataskyddsförordningen. Analysen avgränsas till två rättsliga gränsytor: dels bevarandet av kundkännedomsuppgifter enligt penningtvättslagstiftningen i relation till principen om lagringsminimering och rätten till radering enligt GDPR, dels begränsningar av

den registrerades rätt till information vid övervakning och rapportering av misstänkta transaktioner. Uppsatsen analyserar om dessa begränsningar är förenliga med artikel 23 GDPR samt uppfyller kraven på hur grundläggande rättigheter får begränsas enligt artikel 52.1 i EU-stadgan.

För att uppfylla syftet avser uppsatsen att besvara följande frågor:

(1) Är bevarandetiden för kundkännedomsuppgifter enligt penningtvättsregelverket förenlig med principen om lagringsminimering och rätten till radering enligt GDPR, och är eventuella ingrepp i den registrerades grundläggande rättigheter förenliga med EU-stadgan?

(2) I vilken utsträckning får den registrerades rätt till information enligt artiklarna 13–14 GDPR begränsas vid övervakning och rapportering av misstänkta transaktioner enligt penningtvättsregelverket, och är begränsningarna förenliga med artikel 23 GDPR och EU-stadgan?

1.3 Avgränsningar

Uppsatsens fokus ligger på penningtvätt i snäv bemärkelse. Finansiering av terrorism behandlas endast i den mån den är integrerad i AML-regelverket och nödvändig för att förstå dess struktur och tillämpningsområde, men utgör inte ett självständigt analysobjekt. Andra dataskyddsrättsliga frågor än de som anges ovan behandlas inte även om sådana kan aktualiseras i ett AML-sammanhang. Detta gäller exempelvis frågor om automatiserat beslutsfattande och profilering enligt artikel 22 GDPR, överföring av personuppgifter till tredjeland samt tillsyns- och sanktions-frågor. Inte heller behandlas frågor om rättsmedel eller skadestånd enligt GDPR eller penningtvättslagstiftning. Rättsligt avgränsas uppsatsen till europeisk och svensk rätt. Analysen tar sin utgångspunkt i det nya europeiska AML-paketet, bestående av AML-förordningen, AML-direktivet samt inrättandet av den europeiska tillsynsmyndigheten, Anti-Money Laundering Authority (AMLA). Det tidigare AML-direktiv behandlas endast i den mån det är nödvändigt för att belysa regelverkets utveckling och bakgrunden till den nuvarande ordningen.

1.4 Metod och material

Uppsatsen bygger på rättsdogmatisk metod, vilket innebär att gällande rätt fastställs genom en analys av vedertagna rättskällor, såsom lagstiftning, förarbeten, rättspraxis och doktrin.[4] När det gäller penningtvätt och dataskydd är lagstiftning den främsta rättskällan. Lagstiftning är bindande medan övriga rättskällor enligt svensk juridisk metod endast är vägledande. Uttalanden i lagförarbeten används främst när det saknas vägledande domstolsavgöranden. Eftersom uppsatsen rör ett område där nationell rätt samverkar med EU-rätt används även en EU-rättslig metod, vilket innebär att även unionsrättsliga källor beaktas vid fastställandet av gällande svensk rätt. Dessa regler måste tolkas i ljuset av EU-rättens företräde, ändamålsenlig tolkning och EU-domstolens praxis.[5] Den EU-rättsliga metoden har stora likheter med svensk juridisk metod, men skiljer sig bland annat från den senare genom att EU-rätten inte i samma utsträckning beaktar förarbeten. EU-domstolens praxis är dessutom bindande för medlemsstaterna. Förarbeten används i begränsad omfattning för att belysa lagstiftarens syfte och systematik i den svenska regleringen, men tillmäts mindre vikt än lagtext och EU-domstolens praxis, särskilt när unionsrättsliga frågor aktualiseras. Juridisk doktrin används för att systematisera rättsläget och fördjupa analysen.[6]

Artikel 52.1 i EU-stadgan reglerar hur de grundläggande rättigheter som föreskrivs i denna får begränsas. Det är därmed nödvändigt att bedöma om AML-regelverkets inskränkningar i dataskyddet är lagstadgade, förenliga med rättighetens väsentliga innehåll samt nödvändiga och proportionerliga i förhållande till målet att bekämpa penningtvätt och finansiering av terrorism.[7] Det rättsliga materialet består huvudsakligen av EU-rättsliga instrument, särskilt dataskyddsförordningen (GDPR) och det nuvarande samt föreslagna AML-regelverket, kompletterat med nationell lagstiftning och EU-domstolens praxis. Därutöver används rättskällor som inte är formellt bindande men har praktisk betydelse i rättstillämpningen, såsom riktlinjer från Europeiska dataskyddsstyrelsen (EDPB).

[4] Aleksander Peczenik, ”*Juridikens teori och metod : en introduktion till allmän rättslära*”, Fritze, 1995.

[5] Ola Zetterquist, ”EU-rättslig metod”, i Christian Dahlman & Lena Wahlberg (red.), *Juridiska grundbegrepp: En vänbok till David Reidhav*, Studentlitteratur, 2019.

[6] Ulf Bernitz m.fl., *”Finna rätt – juridikens källmaterial och arbetsmetoder*”, uppl. 16, Norstedts Juridik, 2023.

[7] Bernitz m.fl., *”Finna rätt*”.

1.5 Disposition

I kapitel 1 redogörs för uppsatsen bakgrund, syfte och frågeställning samt de avgränsningar som gjorts. Vidare, så presenteras den metod och det material som ligger till grund för undersökningen.

Kapitel 2 behandlar penningtvättsregelverket (AML) inom EU och svensk rätt. I kapitlet redogörs för regelverkets utveckling och struktur samt för de centrala skyldigheter som åvilat verksamhetsutövare, särskilt avseende kundkännedom, löpande övervakning och rapportering samt dokumentations- och bevarandekrav.

I kapitel 3 behandlas dataskyddsförordningen (GDPR) och dess tillämplighet i ett penningtvättsrättsligt sammanhang. Kapitlet redogör för förordningens syfte, systematik och grundläggande principer samt för de registrerades rättigheter. Särskilt behandlas principen om lagringsminimering, rätten till information samt möjligheterna att begränsa dessa rättigheter enligt artikel 23 GDPR och artikel 52.1 i EU:s stadga om de grundläggande rättigheterna.

Kapitel 4 innehåller en analys av förhållandet mellan AML-regelverkets krav på personuppgiftsbehandling och GDPR:s skydd för den personliga integriteten. Analysen fokuserar huvudsakligen på bevarandetider för kundkännedomuppgifter samt sekretessundantag från informationsskyldigheten. I kapitlet prövas dessa inskränkningar mot unionsrättens krav på bland annat nödvändighet och proportionalitet i enlighet med EU-stadgan.

Uppsatsen avslutas med kapitel 5, där de slutsatser som dragits under analysen sammanfattas och knyts samman. Här presenteras en slutgiltig bedömning av hur spänningsfältet mellan effektiv brottsbekämpning och individens integritetsskydd kan hanteras inom ramen för gällande och kommande rätt.

2 Penningtvättregelverket

2.1 Penningtvätt som samhällsproblem

Ur ett lekmannaperspektiv kan penningtvätt framstå som ett marginellt fenomen, förbehållet en snäv krets kriminella aktörer snarare än ett allvarligt samhällsproblem. I realiteten rör det sig dock om en verksamhet av betydande omfattning med långtgående konsekvenser för den finansiella stabiliteten. Även om penningtvätt till sin natur är svår att kvantifiera med full precision uppskattar internationella organisationer att mellan 715 och 1 670 miljarder euro tvättas årligen, vilket motsvarar cirka 2–5 procent av den globala bruttonationalprodukten.[8]

Mot denna bakgrund har ett omfattande preventivt regelverk utvecklats där privata aktörer tilldelats en central roll att identifiera, övervaka och rapportera misstänkta förhållanden. Denna ordning innebär samtidigt att betydande mängder personuppgifter behandlas inom ramen för penningtvättsregelverket, vilket aktualiserar frågor om dess förhållande till dataskyddsrätten (se kapitel 3). När begreppet AML-regelverket används i denna uppsats avses den reglering som följer av EU:s penningtvättsdirektiv och den svenska penningtvättslagen. Regelverket ålägger finansiella verksamhetsutövare samt vissa icke-finansiella aktörer att identifiera och bedöma risker, uppnå tillräcklig kundkännedom samt övervaka och rapportera misstänkta transaktioner.

Systemet vilar på ett riskbaserat förhållningssätt och innefattar bland annat krav på kundkännedom (Know Your Customer, KYC), löpande övervakning samt dokumentations- och bevarandeskyldigheter enligt 2–5 kap. penningtvättslagen. Dessa bildar tillsammans en sammanhängande struktur som möjliggör tillsyn och kontroll inom penningtvättsregelverket.[9]

Inom sektorn för finansiell teknologi (fintech) och digitala finansiella tjänster aktualiseras AML-regelverket på ett särskilt tydligt sätt. Digitaliserade betalningsflöden och gränsöverskridande transaktioner har förändrat riskbilden för penningtvätt samtidigt som tekniska lösningar möjliggör mer automatiserad riskbedömning och transaktionsövervakning. För dessa aktörer är AML-regelverket därmed inte endast

[8] Prop. 2016/17:173, ”En effektivare bekämpning av penningtvätt”, 2017, s. 58; Europeiska kommissionen, ”Commission Staff Working Document – Supranational Risk Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Union”, SWD(2019) 650 final, 2019, s. 2.

[9] Prop. 2016/17:173, s. 55 f.

en rättslig skyldighet utan en integrerad del av verksamhetens riskhantering och regelefterlevnad. Denna utveckling förstärker samtidigt den omfattande behandling av personuppgifter som sker inom ramen för AML-systemet och tydliggör spänningsförhållandet till dataskyddsrätten.

Mot denna bakgrund behandlas i detta kapitel AML-regelverkets utveckling, centrala skyldigheter för verksamhetsutövare samt regler om dokumentation, bevarande och informationsbegränsningar, i syfte att skapa en systematisk grund för den efterföljande analysen av dess förenlighet med dataskyddsförordningen och de krav som följer enligt artikel 52.1 i EU-stadgan.

För att förstå regelverkets utformning och de ingrepp som denna kan medföra i den personliga integriteten krävs en definition av penningtvätt.[10] Enligt Ekobrottsmyndigheten avser penningtvättåtgärder som syftar till att dölja sambandet mellan ett brott (predikatbrottet) och de medel som genererats genom brottet.[11] Ett typiskt tillvägagångssätt är att illegala medel införlivas i en till synes legitim verksamhet för att dessa ska framstå som lagliga. I denna uppsats riktas dock fokus i första hand mot mer komplexa former av penningtvätt, såsom skiktning (layering), där kapital förflyttas genom flera transaktioner och jurisdiktioner i syfte att försvåra spårbarhet och dölja medlens ursprung.

2.2 Utvecklingen av AML-regelverket

Arbetet mot penningtvätt har vuxit fram gradvis i Europa och Sverige under mer än tre decennier och präglas av ett nära samspel mellan internationella standarder, EU-rättslig och nationell lagstiftning. En genomgående utvecklingslinje har varit en successiv skärpning av kraven på riskbedömning, öppenhet och informationshantering.[12]

EU:s första penningtvättsdirektiv, som byggde på rekommendationer från Financial Action Task Force (FATF), riktade sig främst till banker och ett begränsat urval av finansiella aktörer och betonade kundkännedom och rapporteringsskyldighet. I Sverige infördes reglerna inledningsvis fragmentariskt genom bankrättsliga och straffrättsliga bestämmelser.

[10] Ekobrottsmyndigheten, ”Penningtvättsbrott”, elektronisk källa, 2025.
[11] Ekobrottsmyndigheten, ”Penningtvättsbrott”, elektronisk källa, 2025.
[12] Prop. 2016/17:173, s. 44 ff.

Det var först genom genomförandet av det andra penningtvättsdirektivet (2001/97/EG) som ett mer sammanhållet svenskt regelverk etablerades genom penningtvättslagen (2001:1227).[13]

Med det tredje penningtvättsdirektivet (3AMLD) infördes ett tydligare riskbaserat angreppssätt och regler om politiskt utsatta personer (PEP), vilket markerade en principiell förskjutning från detaljreglering till riskstyrning.[14] Denna utveckling förstärktes genom det fjärde penningtvättsdirektivet, särskilt genom kraven på riskbedömning i artikel 8 i direktiv (EU) 2015/849 (4AMLD).[15] Det tredje direktivet genomfördes huvudsakligen genom justeringar i befintlig lagstiftning och innebar därför ingen genomgripande omstrukturering av det svenska regelverket.[16]

De mest genomgripande förändringarna inom EU:s penningtvättsregler kom 2015 respektive 2018 genom det fjärde och femte penningtvättsdirektivet (5AMLD). Dessa direktiv skärpte kraven på riskbedömning, öppenhet och informationshantering, bland annat genom regler om verkliga huvudmän, centrala register och utvidgade krav på kundkännedom, särskilt i förhållande till digitala tjänster och gränsöverskridande transaktioner.[17] Dessa reformer föranledde införandet av den nya penningtvättslagen (2017:630), som i dag utgör den centrala svenska implementeringen av EU:s fjärde och femte penningtvättsdirektiv. Lagen kompletteras av förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsförordningen) och myndighetsföreskrifter, särskilt från Finansinspektionen, vilka preciserar verksamhetsutövarnas skyldigheter.[18]

Under de senaste åren har EU tagit ytterligare steg mot harmonisering genom det så kallade AML-paketet, bestående av det sjätte penningtvättsdirektivet (direktiv (EU) 2024/1640) och den nya förordningen om åtgärder mot penningtvätt (förordning (EU) 2024/1624), som är direkt tillämplig i medlemsstaterna.[19] Syftet är att skapa ett mer enhetligt och harmoniserat regelverk och minska skillnaderna mellan nationella implementeringar. I Sverige har detta lett till betänkandet SOU 2024:58, som föreslår

[13] Europaparlamentets och rådets direktiv 2001/97/EG, ”om ändring av rådets direktiv 91/308/EEG om åtgärder för att förhindra att det finansiella systemet används för tvättning av pengar”, 2001; SOU 2022:58, ”Skärpta regler om kundkännedom”, s. 45–46.

[14] Direktiv 2005/60/EG, ”Tredje penningtvättsdirektivet”, 2005.

[15] Europaparlamentets och rådets direktiv (EU) 2015/849, *”om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism”*, 2015, art. 8.

[16] SOU 2022:58, ”*Skärpta regler om kundkännedom*”, 2022, s. 45–46.

[17] Direktiv (EU) 2015/849, ”Fjärde penningtvättsdirektivet”, 2015; Direktiv (EU) 2018/843, ”Femte penningtvättsdirektivet”, 2018.

[18] Finansinspektionen, FFFS 2017:11, *Åtgärder mot penningtvätt och finansiering av terrorism*.

[19] Förordning (EU) 2024/1624 (AMLR); Direktiv (EU) 2024/1640 (6AMLD). Se även Europaparlamentets och rådets förordning (EU) 2024/1620 om inrättande av en myndighet för bekämpning av penningtvätt (AMLA).

en ny penningtvättslag som ska ersätta 2017 års lag och genomföra 6AMLD. Genom EU:s AML-paket har harmoniseringen tagit ett avgörande steg. Paketet består bland annat av förordning (EU) 2024/1624 (AMLR), som genom sin direkta tillämplighet skapar ett enhetligt regelverk, samt det sjätte penningtvättsdirektivet (direktiv (EU) 2024/1640). Ett centralt inslag i reformen är inrättandet av den europeiska myndigheten för bekämpning av penningtvätt, AMLA, som har getts en central roll i den direkta tillsynen över vissa gränsöverskridande finansiella institut med hög risk.[20]

2.3 Verksamhetsutövare och tillämpningsområde

AML-regelverket har ett brett tillämpningsområde och omfattar i dag ett stort antal aktörer. Enligt 1 kap. 1 § penningtvättslagen (2017:630) syftar regleringen till att förebygga och förhindra att finansiell verksamhet utnyttjas för penningtvätt eller finansiering av terrorism.[21] Även om dessa företeelser behandlas parallellt i lagstiftningen avgränsas denna framställning till åtgärder mot penningtvätt (se avsnitt 1.3). Finansiering av terrorism berörs endast i den mån det är nödvändigt för att förstå regelverkets systematik.

Kretsen av verksamhetsutövare definieras i 1 kap. 2 § penningtvättslagen och omfattar såväl traditionella finansiella institut som vissa icke-finansiella aktörer. Förutom banker och kreditinstitut – vilka står i fokus för denna uppsats – omfattas bland annat betalningsinstitut, institut för elektroniska pengar, vissa värdepappersföretag, försäkringsförmedlare samt professionella tjänsteutövare såsom advokater, revisorer och fastighetsmäklare. Uppräkningen illustrerar regelverkets stora räckvidd och dess syfte att omfatta de sektorer där risker för penningtvätt typiskt sett uppstår.[22]

Genom regleringen åläggs dessa verksamhetsutövare ett självständigt ansvar att identifiera och bedöma risker, uppnå tillräcklig kundkännedom samt övervaka och rapportera misstänkta förhållanden till behöriga myndigheter (se särskilt 2–6 kap. penningtvättslagen).[23] Systemet vilar på ett riskbaserat förhållningssätt, vilket innebär att åtgärdernas omfattning och intensitet ska anpassas efter verksamhetens art, kundkrets och transaktionsmönster. Ansvaret placeras därmed nära de verksamheter där riskerna uppstår.

[20] Förordning (EU) 2024/1624 (AMLR); Direktiv (EU) 2024/1640 (6AMLD). Se även förordning (EU) 2024/1620 om inrättande av AMLA. För svenskt genomförande, se SOU 2025:22.

[21] Jfr SOU 2024:58, s. 904–905.

[22] Se Finansinspektionen, FFFS 2017:11.

[23] SOU 2024:58, s. 905; se även Direktiv (EU) 2015/849, ”Fjärde penningtvättsdirektivet”, 2015, art. 7–8; Europeiska kommissionen, ”Förslag till penningtvättsförordning”, COM(2021) 420 final, 2021.

Det riskbaserade angreppssättet konkretiseras genom de centrala skyldigheter som behandlas i det följande, särskilt reglerna om kundkännedom, löpande övervakning och rapportering av misstänkta förhållanden, vilka utgör kärnan i det preventiva AML-systemet.

2.3.1 Kundkännedom

Kundkännedom, på engelska "Know Your Customer" (KYC), är en av de mest centrala skyldigheterna för verksamhetsutövare inom AML-lagstiftningen. Syftet med KYC är att säkerställa att aktörer kan identifiera och verifiera sina kunder, förstå deras affärsverksamhet och bedöma risken för penningtvätt (1 kap. 2 §; 4 kap. 6–7 §§ penningtvättslagen). Genom KYC kan misstänkta aktiviteter upptäckas och rapporteras i tid, vilket är avgörande för systemets effektivitet.[24] Den omfattande informationsinsamlingen innebär dock att verksamhetsutövaren bygger upp detaljerade kundprofiler. Här uppstår en inneboende spänning mellan AML:s krav på djupgående kundkännedom och GDPR:s principer om uppgiftsminimering och ändamålsbegränsning, eftersom insamlingen av personuppgifter måste stå i proportion till det eftersträvade syftet.

I praktiken ska verksamhetsutövaren inhämta och dokumentera följande uppgifter (4 kap. 6 § penningtvättslagen): Kundens identitet och kontaktuppgifter, Verklig huvudman (Ultimate Beneficial Owner, UBO), Syftet med affärsrelationen, Kundens ekonomiska profil och typ av transaktioner. KYC är inte en statisk skyldighet utan ska tillämpas enligt ett riskbaserat tillvägagångssätt.[25] Verksamhetsutövaren ska genomföra en initial riskbedömning av varje kund och fortlöpande anpassa övervakningen utifrån identifierad risknivå. Lågriskkunder genomgår enklare kontroller, medan högriskkunder kräver mer omfattande verifiering och dokumentation (4 kap. 7 § penningtvättslagen). Den riskbaserade metodiken är ett centralt verktyg för att uppfylla AML:s mål på ett proportionerligt och resurseffektivt sätt. KYC-kraven gäller i princip alla kunder, men informationsinsamlingens omfattning anpassas efter risknivå. Mer detaljerad information krävs exempelvis för politiskt utsatta personer (Politically Exposed Person, PEP) eller kunder med hög riskprofil, såsom internationella företag med komplexa ägarstrukturer.[26]

[24] SOU 2024:58 s. 904–905.

[25] Direktiv (EU) 2015/849 (4AMLD), art. 8; SOU 2024:58, s. 905.

[26] Direktiv (EU) 2015/849 (4AMLD), art. 3 samt art. 13–14.

Digitalisering och framväxten av fintech-lösningar har gjort KYC-processen mer komplex. Fjärrverifieringar och digital identifiering medför både nya möjligheter och risker, bland annat avseende säkerheten för personuppgifter och risk för identitetsbedrägeri.[27] Detta understryker vikten av att verksamhetsutövare inte bara samlar in korrekt information utan att dessa också säkerställer att uppgifterna lagras och hanteras säkert och effektivt. KYC är därför direkt relevant för analysen av GDPR, eftersom insamling och lagring av omfattande personuppgifter kan stå i konflikt med principen om dataminimering och rätten till radering (art. 5.1 c och e samt art. 17 GDPR). I kapitel 4 kommer KYC:s krav på långvarig dokumentation och detaljerad profilering att prövas mot artiklarna 13–17 GDPR och de krav som följer av artikel 52.1 i EU-stadgan.

2.3.2 Löpande övervakning och rapportering

Löpande övervakning av kundrelationer och transaktioner är en av AML-regelverkets mest centrala skyldigheter och syftar till att upptäcka och reagera på misstänkt penningtvätt eller finansiering av terrorism (4 kap. 6 § penningtvättslagen).[28] Verksamhetsutövare får inte enbart förlita sig på den initiala kundkännedomen, utan måste kontinuerligt analysera finansiell aktivitet för att identifiera avvikelser i beteenden, transaktionsmönster och annan relevant information under hela affärsrelationens löptid. Kravet återfinns både i svensk lag och i EU:s AML-ramverk, som ställer krav på att finansiella institut implementerar kontroller för att upptäcka ovanliga eller potentiellt misstänkta transaktioner (4 kap. 6 § penningtvättslagen).[29]

Övervakningen är riskbaserad. Intensiteten och omfattningen av kontrollerna anpassas efter den bedömda risken för penningtvätt.[30] Transaktioner eller relationer med hög risk, exempelvis sådana som avviker från kundens normala beteendemönster, ska granskas mer noggrant och oftare än de som bedöms ha låg risk. Övervakningen ska vara kontinuerlig, där information om kundens beteende uppdateras och omvärderas i takt med ny tillgänglig information (4 kap. 2 § penningtvättslagen).[31]

När verksamhetsutövaren identifierar en misstänkt transaktion eller aktivitet uppstår en skyldighet att rapportera detta till den nationella finansunderrättelsetjänsten.

[27] SOU 2022:58 s. 145–150 (avsnitt 8.3–8.4).

[28] SOU 2023:58, s. 906 (avsnitt 19.2.2).

[29] Finansinspektionen, ”Riskbaserat förhållningssätt och kundkännedom”, vägledning, elektronisk källa, 2022. [30] Direktiv (EU) 2024/1640, ”Sjätte penningtvättsdirektivet”, 2024, art. 7–8.

[31] SOU 2024:58, s. 904–905 (avsnitt 19.1–19.2).

I Sverige sker detta genom en "Suspicious Activity Report" (SAR) eller "Suspicious Transaction Report" (STR) till Finanspolisen (4 kap. 3 § penningtvättslagen). Rapporten ska innehålla uppgifter om kunden, transaktionen och skälen till misstanken. Rapportering kräver inte bevis för ett faktiskt brott, utan grundas på rimlig misstanke, vilket gör processen både proaktiv och omfattande. Rapporteringen omfattas av en sträng tystnadsplikt och ett lagstadgat meddelandeförbud, vilket syftar till att förhindra att den berörda kunden får kännedom om granskningen (s.k. tipping-off). Detta innebär ett meddelandeförbud som innebär att verksamhetsutövaren inte får informera kunden om att en misstänkt aktivitet har rapporterats eller att en utredning pågår, eftersom detta kan störa utredningen eller leda till att bevisning manipuleras (4 kap. 9 § penningtvättslagen).[32]

Det är just i spänningsfältet mellan denna tystnadsplikt och kraven på dataskydd som de största utmaningarna uppstår. I praktiken innebär övervaknings- och rapporteringsskyldigheten att stora datamängder om kundens finansiella beteende behandlas, analyseras och lagras (4 kap. 2 § penningtvättslagen).[33] Detta gör löpande övervakning till en av AML-regelverkets mest integritetskänsliga delar. Eftersom verksamhetsutövare regelbundet behandlar och analyserar personuppgifter för att upptäcka misstänkt aktivitet uppstår en potentiell konflikt med GDPR:s krav på information, öppenhet och registrerades rätt till skydd av sina personuppgifter enligt EU-stadgan. Särskilt relevant är att AML-reglerna förbjuder att kunden informeras om övervakning eller rapportering, vilket normalt skulle aktivera informationsskyldigheten enligt artiklarna 13–14 GDPR.

Frågan om dessa sekretessundantag är förenliga med GDPR och artikel 52.1 i EU-stadgan är därför central för analysen i kapitel 4. Rapporteringsskyldigheten kräver att verksamhetsutövaren utför en komplex rättslig balansgång. Å ena sidan riskerar aktören sanktioner från Finansinspektionen om kontroller brister eller rapportering uteblir. Å andra sidan kan för omfattande övervakning och rapportering hota kundens integritet, vilket kan strida mot GDPR. Denna regelefterlevnadsutmaning tvingar den finansiella aktören till noggranna rättsliga avvägningar, där felsteg i endera riktningen kan få allvarliga konsekvenser, antingen genom myndighetsåtgärder eller rättsliga anspråk från den registrerade.

[32] Prop. 2003/04:156, s. 53–55.

[33] Finansinspektionen, *Erfarenheter från penningtvättsrapporteringen*, rapport, elektronisk källa, 2024, s. 12.

2.4 Dokumentation och lagring inom AML

Dokumentationskraven inom AML utgör en av de mest ingripande skyldigheterna för verksamhetsutövare, eftersom de direkt påverkar hur stora mängder personuppgifter som hanteras och lagras över tid. Syftet med dokumentationsplikten är att säkerställa att myndigheter vid behov kan rekonstruera transaktioner, verifiera kundens identitet och följa de beslutsunderlag som legat bakom riskklassificeringar och kundkännedomsåtgärder. EU:s penningtvättsdirektiv och den svenska penningtvättslagen kräver systematiskt bevarande av uppgifter som rör kundkännedom, affärsrelationens syfte, transaktioner samt det löpande övervakningsarbetet.

Enligt artikel 40 i det femte penningtvättsdirektivet (EU) 2018/843 ska medlemsstaterna säkerställa att uppgifter som inhämtas genom KYC och övervakning bevaras i minst fem år efter affärsrelationens upphörande. Detta har införlivats i svensk rätt genom 5 kap. 3 § penningtvättslagen, där verksamhetsutövare är skyldiga att bevara dokumentation minst fem år, med möjlighet till förlängning med ytterligare fem år om det bedöms nödvändigt för att förebygga, upptäcka eller utreda penningtvätt eller finansiering av terrorism.

Direktivet och den svenska lagen anger dock att uppgifter inte får lagras längre än nödvändigt. Förlängningar måste vara “strikt nödvändiga” och generella, rutinmässiga förlängningar är inte tillåtna. Bestämmelsen är kopplad till GDPR:s princip om lagringsminimering (artikel 5.1 e GDPR) , som kräver att personuppgifter inte bevaras längre än vad som är nödvändigt med hänsyn till det ursprungliga ändamålet. I teorin är regelverken förenliga: AML anger en minimitid, medan GDPR kräver individuell proportionalitetsbedömning. I praktiken uppstår dock ofta en konflikt mellan dessa krav. Flera studier har påpekat att AML-regelverket i praktiken leder till långvarig lagring av känsliga uppgifter, även när risken är låg och kunden inte längre har en aktiv relation med verksamhetsutövaren. Norska Datatilsynet och Europaparlamentet har i rapporter lyft fram att AML-data ofta hamnar i “osynliga datalager”, där dessa bevaras längre än nödvändigt. Detta beror dels på osäkerhet kring myndighetskrav, dels på rädsla för sanktioner vid bristfällig dokumentation. Den femåriga huvudregeln blir därmed i praktiken ett golv snarare än ett tak, vilket riskerar att komma i konflikt med GDPR:s krav på motiverade och individuellt anpassade lagringstider. Det centrala rättsliga problemet är att AML kräver bevarande av kund- och transaktionsuppgifter även när de inte längre är aktuella, medan GDPR föreskriver radering när ändamålet uppfyllts.

AML-regleringens långsiktiga syfte är att möjliggöra myndighetskontroll även flera år efter misstänkta transaktioner. Därmed bygger AML per definition på en typ av datalagring som i andra sammanhang skulle betraktas som oproportionerlig enligt dataksyddsrätten. Ytterligare komplikationer uppstår eftersom tillsynsmyndigheter, såsom Finansinspektionen, ställer höga krav på spårbarhet och dokumentation. Detta skapar incitament för verksamhetsutövare att lagra mer data än nödvändigt för att undvika sanktioner. Finansinspektionens praxis, där brister i dokumentation ofta anses allvarliga, har bidragit till en överlagringskultur. Ur dataskyddsperspektiv är detta riskabelt, eftersom överskottslagring inte kan motiveras med "för säkerhets skull", utan måste kopplas till ett specificerat AML-ändamål.

2.5 Informationsskyldighet och sekretess

Informationsskyldigheter är en grundläggande del av EU:s dataskyddsreglering och syftar till att ge den registrerade insyn i hur och varför personuppgifter behandlas. Enligt artiklarna 13 och 14 GDPR ska den registrerade informeras om bland annat behandlingsändamål, rättslig grund, lagringstid och de rättigheter som följer av förordningen. Öppenhetsprincipen är central för dataskyddsrätten och förutsätter att den registrerade kan utöva sina rättigheter på ett meningsfullt sätt.[34]

AML-regelverket står i direkt kontrast till denna logik. Eftersom penningtvättsbekämpning bygger på diskret övervakning, myndighetssamverkan och rapportering av misstänkta aktiviteter (SAR/STR), får kunden i många fall inte informeras om att en behandling sker eller att misstanke rapporterats. Detta framgår av artikel 32 i det fjärde penningtvättsdirektivet, som förbjuder verksamhetsutövare att röja för kunden att en rapportering har upprättats eller att en utredning kan pågå. Samma princip återfinns i 3 kap. 3 § penningtvättslagen, som föreskriver att verksamhetsutövaren varken får informera kunden eller tredje man om att rapportering enligt lagen har skett.[35]

Ett motsvarande undantag finns i artikel 14.5 b GDPR, som anger att informationsskyldigheten kan begränsas om den är "omöjlig" eller "skulle medföra en oproportionerlig ansträngning", eller när informationen riskerar att "omöjliggöra eller avsevärt försvåra syftet med behandlingen".

[34] Integritetsskyddsmyndigheten, *Personuppgifter i penningtvättsrapporteringen – sekretess och GDPR*, rapport, elektronisk källa, 2022, s. 8–9.

[35] Finansinspektionen, *Erfarenheter från penningtvättsrapporteringen*, s. 12.

AML-förordningen om harmoniserade sekretessbestämmelser bygger på samma idé: effektiv tillsyn och rapportering kräver att verksamhetsutövaren agerar utan att kunden får vetskap om misstankar eller övervakning.[36] Detta innebär att AML etablerar en strukturell insynsbegränsning som tydligt avviker från GDPR:s normalmodell. Kunden kan inte förstå eller kontrollera sina uppgifter och kan inte utöva sin rätt till rättelse, begränsning eller radering för uppgifter som hen inte vet om att de existerar, trots att dessa uppgifter är några av de mest integritetskänsliga inom finanssektorn. Undantagen från informationsskyldigheten blir därför centrala för analysen av om AML-regleringen överensstämmer med artikel 52.1 i EU-stadgan.[37]

Ett centralt problem är att AML:s sekretessundantag saknar individuell prövning på kundnivå. Undantaget gäller generellt för alla kunder och situationer där övervakning eller rapportering kan bli aktuell. I dataskyddsrätten bygger undantag vanligen på konkreta riskbedömningar, men AML tillåter ett automatiskt "blanket exception". Europaparlamentet och flera nationella dataskyddsmyndigheter har kritiserat detta som potentiellt oproportionerligt, särskilt i kombination med långvarig lagring (jfr 5 kap. 3 § penningtvättslagen).[38]

Samtidigt måste sekretessundantaget förstås i ljuset av AML:s övergripande syfte. Penningtvättsbekämpning är beroende av att misstänkta transaktioner kan rapporteras utan risk för undanröjande av bevis, förändrade beteenden eller aktivt motstånd från kunden. Verksamhetsutövare får därför inte "varna" kunden, eftersom detta skulle undergräva systemets effektivitet.[39] EU-rätten accepterar därför långtgående undantag från informationsplikten, som i andra sammanhang vore ovanliga. Frågan är således inte om AML kräver sekretess, utan om dagens generella och oinskränkta sekretessundantag verkligen uppfyller EU-stadgans krav på nödvändighet och proportionalitet.[40] Proportionalitetsprincipen kräver att begränsningar av grundläggande rättigheter inte får gå längre än vad som är absolut nödvändigt. Två centrala problem uppstår: Om undantaget är för brett i förhållande till behovet samt om det saknas tillräckliga kontrollmekanismer som förhindrar att undantaget används i fler situationer än nödvändigt. Dessa spänningar mellan AML:s sekretesskrav och GDPR:s öppenhetsprincip utgör en av de mest centrala rättsliga konflikterna (se vidare kapitel 4).

---

[36] Integritetsskyddsmyndigheten (IMY), *Personuppgifter i penningtvättsrapporteringen – sekretess och GDPR*, s. 10–11.

[37] Ulf Bernitz, *"EU:s stadga om de grundläggande rättigheterna – En kommentar*", Norstedts Juridik, 202.

[38] Finansinspektionen, *Erfarenheter från penningtvättsrapporteringen*, s. 15; SOU 2024:58, s. 51 ff.

[39] Finansinspektionen, *Erfarenheter från penningtvättsrapporteringen*, s. 1; Integritetsskyddsmyndigheten, *Personuppgifter i penningtvättsrapporteringen – sekretess och GDPR*, s. 12.

[40] Bernitz, *"EU:s stadga", s. 220; Integritetsskyddsmyndigheten*, "*Personuppgifter i penningtvättsrapporteringen*", s. 14.

2.6 Proportionalitet i AML-regleringen

Arbetet mot penningtvätt och finansiering av terrorism vilar på en grundläggande rättspolitisk premiss: att integriteten i det finansiella systemet utgör ett överordnat allmänintresse, vilket motiverar långtgående åtgärder gentemot enskilda aktörer och individer.[41] Detta framgår tydligt både av EU-rättens och den svenska lagstiftarens motiveringar till de successivt ökande kraven inom AML-området. Redan i det fjärde penningtvättsdirektivet framhålls att bekämpningen av penningtvätt är ”väsentlig för unionens finansiella stabilitet och säkerhet”.[42] Motsvarande resonemang återfinns i det nya AML-paketet, där lagstiftaren uttryckligen framhåller att en hög grad av harmonisering är nödvändig för att undvika regelkonflikter och säkerställa att unionsrättens skyddsintressen får genomslag i praktiken (skäl 7–10, AMLR).[43]

AML-regleringen konstrueras således som ett riskpreventivt system, där integritetsintrång i form av omfattande databehandling, rapporteringsskyldigheter och begränsad öppenhet i vissa situationer anses vara nödvändiga för att uppnå regelverkets syfte. Svensk lagstiftning ansluter sig till samma argumentationslinje. I förarbetena till 2017 års penningtvättslag anges att åtgärderna måste vara “tillräckligt långtgående för att effektivt förhindra att det finansiella systemet missbrukas”, även om de innebär inskränkningar i den personliga integriteten. 2022 års penningtvättsutredning bygger vidare på detta resonemang och framhåller att den direkta rättsliga styrningen från EU, bland annat genom 6AMLD och AMLR, kräver att Sverige anpassar sin reglering för att uppnå “ett funktionsdugligt och effektivt AML-system”.[44]

I detta sammanhang blir proportionalitet ett centralt begrepp. Enligt EU-stadgans artikel 52.1 får grundläggande rättigheter, såsom rätten till skydd för personuppgifter enligt artikel 8 i stadgan, begränsas under förutsättning att detta sker genom lag, respekterar rättighetens väsentliga innehåll samt är nödvändig och proportionerlig i förhållande till det eftersträvade målet.[45] AML-regelverket bygger på antagandet att penningtvättsbekämpning utgör ett legitimt mål av allmänintresse, vilket kan motivera mer långtgående intrång än vad som normalt skulle anses acceptabelt.

[41] Finansinspektionen, *Erfarenheter från penningtvättsrapporteringen*, s. 20–22.

[42] Europaparlamentets och rådets direktiv (EU) 2015/849 (4AMLD), skäl 1.

[43] Förordning (EU) 2024/1624 (AMLR), skäl 7–10.

[44] SOU 2024:58, s. 51 ff.

[45] Bernitz, ”*EU:s stadga*”, s. 225–239; Integritetsskyddsmyndigheten, *”Personuppgifter i penningtvättsrapporteringen*”, s. 15–16.

Detta blir särskilt tydligt avseende längre lagringstider, omfattande kundkännedom och undantag från informationsskyldigheten, vilka enligt lagstiftaren inte endast är funktionellt nödvändiga utan även proportionerliga, då de riktar sig mot aktörer och situationer med förhöjd risk. Proportionalitetsbedömningen ska dock förstås som villkorad och kontextberoende, där varje ingrepp måste stå i rimlig proportion till det riskbaserade syftet.

3 GDPR i ljuset av penningtvätt

3.1 GDPR:s tillämplighet inom AML

Den allmänna dataskyddsförordningen (EU) 2016/679 (GDPR) utgör det centrala rättsliga ramverket för skyddet av personuppgifter inom Europeiska unionen och började tillämpas den 25 maj 2018. Förordningen syftar dels till att stärka skyddet för den registrerades grundläggande rättigheter och friheter, dels till att säkerställa en enhetlig reglering av personuppgiftsbehandling inom EU.

Syftet kommer tydligt till uttryck i artikel 1 GDPR, där det anges att förordningen ska skydda fysiska personers grundläggande rättigheter och friheter, särskilt rätten till skydd av personuppgifter, samtidigt som det fria flödet av personuppgifter inom unionen inte ska begränsas. Dessa intressen har även en tydlig förankring i EU:s primärrätt. Artikel 7 i EU-stadgan skyddar rätten till respekt för privat- och familjeliv, medan artikel 8 uttrycker rätten till skydd av personuppgifter. GDPR kan därmed förstås som ett instrument som konkretiserar dessa grundläggande rättigheter, vilket innebär att förordningen ska tolkas i ljuset av stadgans bestämmelser.[46]

Systematiskt är GDPR uppbyggd kring de grundläggande principerna för personuppgiftsbehandling i artikel 5, såsom laglighet, ändamålsbegränsning, uppgiftsminimering, lagringsminimering och öppenhet. Dessa principer genomsyrar både skyldigheterna för den personuppgiftsansvarige, den organisation eller myndighet som bestämmer ändamålen och medlen för behandlingen, och rättigheterna för den registrerade, det vill säga den levande fysiska person som uppgifterna avser. Förordningen fastställer även de rättsliga grunderna för laglig behandling i artikel 6, samt möjligheten att genom nationell lagstiftning begränsa vissa rättigheter enligt artikel 23.

Av särskild betydelse för denna uppsats är att GDPR är tillämplig på den person uppgiftsbehandling som banker och andra finansiella institut utför för att uppfylla

[46] Integritetsskyddsmyndigheten (IMY), *GDPR – Syfte och tillämplighet*, elektronisk källa, 2026.

skyldigheter enligt penningtvättsregelverket, exempelvis vid kundkännedomsåtgärder, transaktionsövervakning och rapportering av misstänkt verksamhet. Detta ska skiljas från behandling som utförs av behöriga myndigheter för brottsbekämpande ändamål, vilken i stället regleras av direktiv (EU) 2016/680 (LED) och den svenska brottsdatalagen (2018:1177). Att AML-arbetet i stor utsträckning genomförs av privata aktörer innebär därför att GDPR som utgångspunkt är fullt tillämplig, trots behandlingens brottsförebyggande karaktär. Detta innebär att den personuppgiftsbehandling som sker inom ramen för penningtvättsregelverket måste bedömas mot bakgrund av GDPR:s systematik och begränsningsregler.

Mot denna bakgrund fokuserar detta kapitel på de bestämmelser i GDPR som är särskilt relevanta för personuppgiftsbehandling som sker för att uppfylla skyldigheter enligt AML-regelverket, särskilt principen om lagringsminimering, rätten till radering samt rätten till information, och hur dessa rättigheter kan inskränkas inom ramen för artikel 23 GDPR.

3.2 Principen om lagringsminimering och rätten till radering

En viktig fråga i relationen mellan GDPR och AML-regelverket rör hur länge personuppgifter får bevaras. Enligt penningtvättslagen är verksamhetsutövare, såsom banker och andra finansiella institut, skyldiga att samla in och lagra omfattande uppgifter om sina kunder, bland annat genom kundkännedomsåtgärder. Dessa uppgifter ska enligt AML-regelverket bevaras under en viss tid efter att affärsförbindelsen har avslutats. Samtidigt uppställer GDPR tydliga krav på att personuppgifter inte får lagras längre än vad som är nödvändigt för de ändamål för vilka de behandlas (se skäl 39 GDPR). Denna spänning aktualiserar framför allt lagringsminimeringsprincipen i artikel 5.1 e GDPR samt den registrerades rätt till radering enligt artikel 17 GDPR. Bestämmelserna utgör centrala uttryck för skyddet av den personliga integriteten och måste därför analyseras när AML-regelverkets krav på lagring prövas mot unionsrättens proportionalitetskrav.[47]

3.2.1 Lagringsminimering och proportionalitet under AML

Principen om lagringsminimering innebär enligt artikel 5.1 e GDPR att personuppgifter inte får bevaras i en form som möjliggör identifiering av den registrerade längre än vad som är nödvändigt för de ändamål för vilka uppgifterna behandlas.

[47] Jfr artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna samt EU-domstolens dom i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland, p. 46–48.

Principen är nära kopplad till ändamålsbegränsningen i artikel 5.1 b GDPR, eftersom lagringstidens längd ska bestämmas med utgångspunkt i behandlingens syfte.[48]

Den nära kopplingen mellan lagringminimering och ändamålsbegränsning blir särskilt tydlig i frågan om ändamålsglidning. När banker samlar in uppgifter för kundkännedomsändamål (Know Your Customer, KYC) uppstår en spänning i förhållande till ändamålsprincipen.[49] Frågan är huruvida personuppgifter som behandlas för att uppfylla en rättslig förpliktelse enligt AML-regelverket också kan användas för bankernas egna kommersiella riskbedömningar, eller om detta innebär en oförenlig vidarebehandling. Frågan om vidarebehandling måste prövas mot de stränga krav på nödvändighet som följer av EU-domstolens praxis. Domstolen har fastställt att kravet på nödvändighet ska tolkas restriktivt; det är inte tillräckligt att en åtgärd är ändamålsenlig eller praktiskt motiverad, utan den måste vara strikt nödvändig och proportionerlig för att uppnå ett mål av allmänt intresse. Denna praxis sätter därmed en yttre gräns för behandlingen av uppgifter som grundar sig på en rättslig förpliktelse.[50] Principen innebär, i enlighet med rättspraxis rörande artiklarna 7 och 8 i EU-stadgan, att en generell och odifferentierad lagring av uppgifter utan koppling till en konkret risk eller misstanke ofta är oförenlig med unionsrätten. Även om denna praxis främst rör elektronisk kommunikation, illustrerar den de stränga krav på rättssäkerhetsgarantier som ställs vid alla former av generella lagringsskyldigheter.[51]

Inom AML-regelverket föreskrivs i dag en generell skyldighet att bevara kundkännedomsuppgifter i minst fem år efter det att affärsförbindelsen har avslutats, med möjlighet till förlängning under vissa omständigheter (5 kap. 3 § penningtvättslagen). Denna typ av generell och förutbestämd lagringstid innebär att personuppgifter lagras oberoende av om någon konkret misstanke om penningtvätt föreligger. I doktrinen har det påpekats att sådana generella lagringsskyldigheter kan stå i spänning med GDPR:s krav på nödvändighets- och proportionalitetsbedömning.[52] Samtidigt erkänns bekämpningen av penningtvätt och finansiering av terrorism som ett viktigt samhällsintresse inom unionsrätten.[53] Principen om lagringsminimering utesluter därför inte att uppgifter bevaras under längre tidutesluter därför inte att uppgifter bevaras under längre tid.

[48] EU-domstolen, mål C-131/12, *Google Spain*, EU:C:2014:317, p. 92–99.

[49] Christopher Kuner m.fl., ”*The GDPR: A Commentary*”, Oxford University Press, 2020, art. 5.1 b. [50] EU-domstolen, *Digital Rights Ireland, s*. 52.

[51] EU-domstolen, förenade målen C-203/15 och C-698/15, *Tele2 Sverige och Watson*, EU:C:2016:970. [52] Kuner m.fl., ”The GDPR: A Commentary”, s. 348 f.

[53] EU-domstolen, *Digital Rights Ireland.*

3.2.2 Rätten till radering och AML:s begränsningar

Rätten till radering, ofta benämnd ”rätten att bli bortglömd”, utgör ett uttryck för den registrerades kontroll över sina personuppgifter. Enligt artikel 17.1 GDPR har den registrerade rätt att få sina personuppgifter raderade utan onödigt dröjsmål när uppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller annars behandlats. Rätten är dock inte absolut. Av artikel 17.3 b GDPR följer att rätten till radering inte gäller i den mån behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige. AML-regelverkets krav på bevarande av kundkännedomsuppgifter utgör just en sådan rättslig förpliktelse (artikel 17.3 b GDPR jämförd med 3 kap. 12 § penningtvättslagen 2017:630). Detta innebär att banker och andra verksamhetsutövare som omfattas av AML-regelverket i regel är förhindrade att radera uppgifter under den föreskrivna lagringstiden, även om den registrerade begär det. EU-domstolen har emellertid understrukit att undantag från grundläggande rättigheter ska tolkas restriktivt och att även behandling som grundas på en rättslig förpliktelse måste uppfylla proportionalitetskravet enligt artikel 52.1 i EU-stadgan.[54] Det innebär att lagringsskyldighetens längd, omfattning och konkreta tillämpning måste kunna motiveras av ett faktiskt behov som inte rimligen kan tillgodoses genom mindre ingripande åtgärder.

I detta sammanhang aktualiseras frågan om generella och långvariga lagringstider är förenliga med kravet på nödvändighet och proportionalitet. Rätten till radering får i detta avseende en indirekt betydelse: även om den kan begränsas genom sektorsspecifik lagstiftning fungerar den som ett normativt riktmärke för hur långtgående lagringskrav får vara.[55]

3.3 Öppenhet och rätten till information under AML

Öppenhet och den registrerades rätt till information utgör grundläggande delar av GDPR och ger uttryck för principen om laglig, korrekt och öppen behandling av personuppgifter enligt artikel 5.1 a GDPR. Principen innebär att den registrerade

[54] EU-domstolen, *Tele2 Sverige*, p. 96–99.
[55] Lee A. Bygrave, ”*Data Protection Law: Approaching Its Rationale, Logic and Limits*”, Kluwer Law International, 2002, s. 154 f.

ska kunna förstå hur, av vem och för vilka ändamål personuppgifter behandlas, vilket är en förutsättning för att faktiskt kunna utöva sina rättigheter och kontrollera behandlingen (skäl 58 GDPR). Utan ett fungerande krav om öppenhet riskerar skyddet av den registrerades integritet att bli mer formellt än reellt, eftersom rättigheter förlorar sin praktiska och effektiva verkan om individen saknar insyn i hur behandlingen sker i praktiken.[56]

I ett AML-sammanhang blir rätten till information och öppenhet särskilt relevant eftersom AML-regelverket förutsätter att stora mängder personuppgifter behandlas i syfte att förebygga och avslöja penningtvätt, något som i sin tur kan komma i konflikt med kravet på öppenhet gentemot den registrerade. För att förstå denna balans är det därför nödvändigt att analysera vilka informationsskyldigheter GDPR ålägger den personuppgiftsansvarige, särskilt vid indirekt insamling av personuppgifter (artiklarna 13 och 14 GDPR).

3.3.1 Principen om öppenhet och informationsskyldigheter i AML

Principen om öppenhet utgör en kärnfråga i GDPR:s personuppgiftsskyddsregim och är uttryckligen fastställd i artikel 5.1 a GDPR, där det anges att personuppgifter ska behandlas "lagligt, korrekt och på ett öppet sätt i förhållande till den registrerade". Principen utgör en grundförutsättning för att den registrerade ska kunna utöva sina rättigheter och förstå hur den egna personliga integriteten påverkas av personuppgiftsbehandling (jfr GDPR, skäl 39).

Principen konkretiseras genom de detaljerade informationsskyldigheter som följer av artikel 12 och kapitel III i GDPR. Dessa bestämmelser bygger på antagandet att faktisk insyn och begriplig information är en förutsättning för ett effektivt skydd av den registrerades grundläggande rättigheter.[57]

Enligt artikel 12 GDPR ska den personuppgiftsansvarige vidta lämpliga åtgärder för att tillhandahålla information och kommunikation i samband med utövandet av den registrerades rättigheter på ett koncist, klart, begripligt och lättillgängligt sätt, med enkelt språk. Informationen ska som huvudregel lämnas utan onödigt dröjsmål och utan kostnad för den registrerade. Detta förstärker GDPR:s fokus på faktisk och praktiskt tillgänglig öppenhet, snarare än enbart formell informationsgivning.[58]

[56] EU-domstolen, *Digital Rights Ireland.*

[57] Bygrave, *"Data Protection Law*", s. 145 ff.

[58] GDPR, art. 12; EDPB, "*Guidelines on transparency*".

De mer detaljerade upplysningsskyldigheterna regleras i artiklarna 13 och 14 GDPR. Artikel 13 är tillämplig när personuppgifter samlas in direkt från den registrerade och omfattar bland annat information om den personuppgiftsansvariges identitet, ändamålen med behandlingen, den rättsliga grunden, mottagare av personuppgifter samt eventuella överföringar till tredjeland. Artikel 14 reglerar motsvarande informationsskyldighet när personuppgifter inte samlas in från den registrerade, exempelvis när uppgifterna hämtas från tredje part eller offentliga register. Informationen ska i sådana fall lämnas inom rimlig tid, i regel senast inom en månad.

Syftet med dessa bestämmelser är att säkerställa att den registrerade inte blir föremål för personuppgiftsbehandling utan insyn samt att möjliggöra förståelse och faktisk kontroll över behandlingar som påverkar den personliga integriteten. Öppenhetsprincipen är därmed nära kopplad till rätten till information och självbestämmande, vilka utgör centrala skyddsvärden i GDPR:s systematik. [59]

I ett AML-sammanhang aktualiserar dock särskilda spänningar i förhållande till kraven om öppenhet. Regelverket om åtgärder mot penningtvätt och finansiering av terrorism kan kräva diskret övervakning, sekretess och begränsad informationsgivning för att inte äventyra brottsutredningar. Detta påverkar hur och när information enligt GDPR kan lämnas till den registrerade och utgör en central konfliktlinje i samspelet mellan AML och dataksyddsrätten.[60]

3.4 Begränsningar av GDPR rättigheter i AML

Även om GDPR ger ett omfattande skydd för den registrerades rättigheter och integritet, är skyddet inte absolut. För att möjliggöra en avvägning mellan individens rättigheter och viktiga samhällsintressen, såsom effektiv brottsbekämpning och bekämpning av penningtvätt, innehåller GDPR bestämmelser som medger begränsningar av vissa rättigheter. Den rättsliga grunden för sådana begränsningar återfinns främst i artikel 23 GDPR, som anger under vilka villkor medlemsstaterna genom lag får begränsa den registrerades rättigheter och friheter. I ett AML-sammanhang är denna begränsningsklausul särskilt relevant, eftersom AML-regelverket ställer krav på lagring av uppgifter, diskret övervakning och tystnadsplikt i syfte att inte äventyra brottsutredningar.

[59] Christopher Kuner, ”Transborder Data Flows and Data Privacy Law”, Oxford University Press, 2013, s. 98 ff. [60] Prop. 2017/18:216, s. 188 ff.

För att förstå hur dessa begränsningar får utformas krävs därför en genomgång av artikel 23 i dess unionsrättsliga kontext samt hur bestämmelsen kommit till uttryck i svensk rätt.

3.4.1 Rättsligt stöd för inskränkningar enligt artikel 23 GDPR

Artikel 23 GDPR utgör en speciell undantagsregel som tillåter medlemsstaterna att begränsa vissa av de rättigheter som GDPR annars garanterar, såsom rätten till information, rätten till tillgång, rätten till radering och andra rättigheter, under förutsättning att vissa strikta kriterier är uppfyllda.[61]

För det första måste begränsningen ha stöd i lag. Detta innebär att det krävs ett tydligt lagstöd som är fastställt genom lagstiftning och som i EU-rättens hierarki måste vara förenligt med primärrätten.[62] Lagstödet ska inte vara allmänt formulerat utan måste vara specificerat med tydligt definierade ändamål, material och tillämpliga behandlingar.[63] Detta krav på klarhet och förutsebarhet speglar GDPR:s kärnprinciper och är centralt för att undvika oskäliga inskränkningar av individens rättigheter. För det andra måste begränsningen syfta till att skydda ett legitimt allmänt intresse eller annat angeläget samhällsintresse. Artikel 23.1 GDPR anger uttryckligen exempel på sådana intressen, däribland förebyggande, utredning och lagföring av brott samt andra viktiga mål av allmänt intresse inom unionen eller en medlemsstat. Bekämpningen av penningtvätt och finansieringen av terrorism faller tydligt inom denna kategori. [64]

Således kan lagstiftaren i ett medlemsland besluta om begränsningar för att tillgodose behovet av effektiv bekämpning av exempelvis penningtvätt och terrorfinansiering, under förutsättning att krav på proportionalitet och nödvändighet är uppfyllda.[65]

Det centrala juridiska kravet på en begränsning enligt artikel 23 är att den ska vara nödvändig och proportionerlig i förhållande till det angivna syftet. Detta innebär att en begränsning inte får gå längre än vad som krävs för att uppnå det legitima målet och att den måste stå i rimlig proportion till de rättigheter som inskränks.

---

[61] EDPB, ”*Guidelines on Article* 23 GDPR.

[62] Peers m.fl., *”Charter Commentary*”, art. 52. [63] fr
EU-domstolen, *Digital Rights Ireland*

[64] Prop. 2017/18:216.

[65] Stadgan, art. 52.1; EU-domstolen, *Schrems II.*

Denna proportionalitetsprincip är i sin tur kopplad till EU-stadgans artikel 52.1, som uttryckligen föreskriver att inskränkningar i rättigheter och friheter bara får ske "om det är nödvändigt och proportionerligt" med hänsyn till det allmänna intresset.

I förarbeten och doktrin betonas att artikel 23 inte får användas för att kringgå GDPR:s huvudprinciper, utan endast för att anpassa dem till specifika och väldefinierade samhällsintressen, såsom brottsbekämpning.[66] Begränsningsklausulen är därför ett verktyg för balans, inte ett undantag från skyddet, och bör alltid tolkas restriktivt i ljuset av den starka skyddsregim som GDPR utgör.

3.4.2 Nationella begränsningar i svensk rätt

I svensk rätt har artikel 23 GDPR legat till grund för införandet av särskilda begränsningar av de registrerades rättigheter, särskilt inom områden som rör brottsbekämpning och tillsyn. Ett tydligt exempel återfinns i penningtvättslagen som innehåller bestämmelser om rapporteringsskyldighet och tystnadsplikt, samt i offentlighets- och sekretesslagen (2009:400), som reglerar sekretess till skydd för brottsutredande verksamhet. Till exempel tillämpas sekretess enligt penningtvättslagens regler om anmälningsskyldighet och förbud mot att avslöja rapporteringsskyldighetens existens gentemot den rapporterade. Syftet är att förhindra att misstänkta aktörer får vetskap om att deras transaktioner eller beteenden är föremål för granskning, vilket skulle kunna undergräva brottsbekämpningens effektivitet.[67] Denna typ av sekretessutformning är ett tydligt exempel på hur artikel 23 GDPR kan komma till uttryck i svensk rätt genom särskilda undantag från insyn och informationsskyldighet.

Samtidigt framgår av doktrin och myndighetsvägledning att gränsdragningen mellan vilken information som kan undanhållas och vilken som ska lämnas inte alltid är tydlig.[68] I vissa situationer aktualiseras frågor om hur långt sekretessen kan sträcka sig i förhållande till de registrerades rättigheter enligt GDPR, särskilt i gränslandet mellan AML-rapportering och den registrerades rätt till insyn i den egna personuppgiftsbehandlingen. Denna spänningsyta utgör en central utgångspunkt för analysen i kapitel 4. Sammanfattningsvis visar de svenska begränsningarna hur artikel 23 GDPR kan tillämpas för att tillgodose viktiga offentligrättsliga intressen,

[66] Kuner m.fl., *GDPR: A Commentary.* [67]
Prop. 2017/18:216, s. 190.
[68] IMY, "GDPR och brottsbekämpning".

såsom brottsbekämpning, utan att i sig upphäva GDPR:s skydd. Tillämpningen kräver dock en noggrann rättslig avvägning, vilket aktualiseras i den fortsatta analysen.

3.5 EU-stadgan och begränsningar av GDPR-rättigheter

För att förstå de rättsliga ramarna för begränsningar av de registrerades rättigheter och proportionalitetsbedömningar i AML-sammanhang måste GDPR ses i ljuset av EU:s stadga om de grundläggande rättigheterna. Stadgan har primär rättsverkan inom EU och är bindande för medlemsstaterna när de tillämpar unionsrätt, vilket innebär att både nationell lagstiftning och förordningar som GDPR måste tolkas i enlighet med stadgans bestämmelser.[69]

Särskilt relevanta är artiklarna 7 och 8 i stadgan, som skyddar rätten till privatliv respektive skyddet för personuppgifter. Dessa bestämmelser utgör den konstitutionella grund som GDPR konkretiserar genom att fastställa principer och rättigheter för personuppgiftsbehandling. Förordningen är tillämplig på privata aktörer, såsom banker och andra finansiella institut, när de behandlar personuppgifter inom ramen för AML-åtgärder, exempelvis vid kundkännedom, transaktionsövervakning och rapportering av misstänkt verksamhet.

Av artikel 52.1 i stadgan följer att grundläggande rättigheter får begränsas om inskränkningen har stöd i lag, tillgodoser ett legitimt allmänintresse och är nödvändig samt proportionerlig i förhållande till det eftersträvade syftet. Motsvarande möjlighet till begränsningar återfinns i artikel 23 GDPR. Bekämpningen av penningtvätt och finansiering av terrorism utgör ett sådant legitimt allmänintresse som kan motivera inskränkningar i exempelvis rätten till radering eller rätten till information.

Den avgörande frågan är emellertid om sådana inskränkningar är proportionerliga. Proportionalitetsbedömningen aktualiserar typiskt sett tre led: vilken rättighet som begränsas, vilket allmänintresse som åberopas samt om inskränkningen är nödvändig och rimligt avvägd i förhållande till det eftersträvade målet. I AML-sammanhang uppstår denna avvägning särskilt i relation till krav på lagring av kunduppgifter och begränsningar av öppenhet genom sekretess och rapporteringsregler.

[69] IMY, ”GDPR och brottsbekämpning”.

Genom att placera GDPR inom EU-stadgans konstitutionella ram etableras därmed den rättsliga utgångspunkt mot vilken AML-regelverkets krav på lagring och sekretess ska prövas. Denna ram ligger till grund för den fortsatta analysen i kapitel 4, där samspelet mellan AML och GDPR bedöms mot bakgrund av unionsrättens proportionalitetskrav.

4 Analys: AML och GDPR i samspel och konflikt

4.1 Analysens utgångpunkter

I detta kapitel sammanförs de två rättsområden som hittills har behandlats separat: regelverket för bekämpning av penningtvätt och ramverket för dataskydd enligt GDPR. Syftet med analysen är att undersöka det spänningsfält som uppstår när bankernas skyldighet att motverka brottslighet kolliderar med individens rätt till personlig integritet. För att göra analysen mer konkret belyses särskilt utmaningarna inom fintech-sektorn. Eftersom fintechbolag ofta bygger sin verksamhet på helt digitala flöden och behandling av stora mängder data, blir konflikterna mellan AML-regelverkets bevarandekrav och GDPR:s dataskyddsprinciper särskilt tydliga inom denna sektor. Analysen tar därför sin utgångspunkt i uppsatsens två frågeställningar: (1) bevarandetidens förenlighet med GDPR:s lagringsminimering och rätten till radering, samt (2) begränsningar av informationsrätten vid övervakning och rapportering. Fintech-sektorn används genomgående som ett konkret exempel för att synliggöra hur spänningarna uppstår i en datadriven och digitaliserad verksamhet.

4.2 Lagringskonflikt mellan AML och GDPR

En central konflikt mellan regelverken rör spänningen mellan AML-lagstiftningens krav på bevarande av uppgifter och GDPR:s princip om lagringsminimering. Enligt 5 kap. 3 § penningtvättslagen är verksamhetsutövare skyldiga att bevara kundkännedomsuppgifter och transaktionsunderlag i minst fem år efter att affärsförbindelsen har upphört. Syftet med denna skyldighet är att säkerställa att brottsbekämpande myndigheter kan genomföra retroaktiva utredningar av finansiell brottslighet. Denna fasta tidsfrist står dock i spänningsförhållande till GDPR:s principer. Enligt artikel 5.1 e GDPR får personuppgifter inte bevaras i en form som möjliggör identifiering av den registrerade längre än vad som är nödvändigt för ändamålen med behandlingen. För den enskilde innebär detta att rätten till radering enligt artikel 17 i praktiken sätts åt sidan så länge den lagstadgade bevarandetiden enligt penningtvättslagen löper. Konflikten blir särskilt tydlig när kundrelationen har upphört: medan GDPR i princip förutsätter att uppgifter raderas när ändamålet upphört, ålägger AML-regelverket verksamhetsutövaren att fortsatt bevara en omfattande informationsmängd om individen.

Bedömningen av om AML-regelverkets lagringskrav är förenliga med unionsrätten måste ske enligt den struktur som följer av artikel 52.1 i EU-stadgan. Detta innebär en prövning i flera led: (i) om inskränkningen har stöd i lag, (ii) om den eftersträvar ett legitimt mål av allmänt intresse, (iii) om åtgärden är nödvändig för att uppnå detta mål, samt (iv) om den är proportionerlig i snäv mening, det vill säga rimligt avvägd i förhållande till intrånget i den enskildes rättigheter.

I AML-kontexten uppstår därmed en rättslig spänning mellan en fast bevarandetid och GDPR:s krav på nödvändighets- och ändamålsstyrd lagring. Medan penningtvättsregelverket föreskriver en generellt tillämplig bevarandetid om fem år (och i vissa fall längre), utgår GDPR från att lagringstid ska vara kopplad till ändamålet och begränsas till vad som är nödvändigt. Frågan blir därför hur regelverken kan tillämpas på ett sätt som är ömsesidigt förenligt, särskilt efter att en kundrelation har upphört. I praktiken kan bevarandetiden få en "slentrianmässig" effekt, där uppgifter lagras längre än vad som är motiverat i det enskilda fallet, inte minst på grund av tillsyns- och sanktionsrisk. För att uppnå förenlighet med unionsrätten behöver lagringen kunna motiveras utifrån ändamål och proportionalitet, och inte enbart ske "för säkerhets skull".[70]

Inom fintech-sektorn förstärks dessa problem ytterligare. Verksamheterna bygger ofta på helt digitala flöden och insamling av stora mängder realtidsdata. Medan traditionella banker historiskt har arbetat med mer avgränsade informationsmängder, genererar fintech-bolag omfattande digitala fotspår genom integrerade tjänster och frekventa transaktioner. Kravet att bevara dessa datamängder i minst fem år innebär en förhöjd integritetsrisk, eftersom både sannolikheten för och konsekvenserna av dataintrång ökar i takt med lagringstidens längd och datamängdens omfattning. För fintech-aktörer, som ofta profilerar sig genom effektivitet och teknologisk innovation, blir kravet att ”låsa” stora mängder data under lång tid en betydande administrativ och teknisk belastning som står i spänningsförhållande till målet om dataminimering. För att bedöma om denna inskränkning är rättsligt försvarbar måste den prövas mot proportionalitetsprincipen i EU-stadgan. Bevarandetiden kan i ett första steg anses vara ägnad att uppnå det legitima målet att bekämpa penningtvättning och finansieringen,

[70] Se EU-domstolens resonemang om nödvändighet och lagringstider i EU-domstolen, *Digital Rights Ireland*, p. 52–54.

eftersom den ger brottsbekämpande myndigheter möjlighet att spåra och analysera komplexa finansiella flöden i efterhand. Nödvändighetsbedömningen är emellertid mer problematisk. Det framstår som tveksamt om en generellt fastställd femårsgräns verkligen är nödvändig för samtliga typer av uppgifter, särskilt i en digital miljö där transaktioner kan analyseras i realtid. I detta sammanhang skulle en mer differentierad lagringsmodell, baserad på kundens riskprofil, kunna utgöra ett mindre ingripande alternativ. För fintech kunder, vars ekonomiska liv ofta är i hög grad digitaliserat, innebär en femårig lagring att en mycket detaljerad bild av deras beteendemönster bevaras hos privata aktörer även efter att kundrelationen har upphört.

Mot denna bakgrund framstår den femåriga lagringsregeln som förenlig med GDPR i sin rättsliga konstruktion, eftersom den vilar på lagstadgad skyldighet och ett legitimt allmänintresse. Däremot aktualiserar den generella och odifferentierade tilllämpningen proportionalitetsproblem, särskilt i förhållande till lågriskkunder. Konflikten ligger således inte i regelns existens, utan i dess praktiska räckvidd. En motsvarande proportionalitetsproblematik uppstår även i fråga om informationsrätten och sekretess, vilket behandlas i följande avsnitt.

4.3 Sekretesskonflikt mellan AML och GDPR

Den andra centrala konfliktytan mellan AML-regelverket och GDPR rör spänningen mellan kravet på sekretess vid övervakning och rapportering av misstänkta transaktioner, å ena sidan, och den registrerades rätt till information och öppenhet enligt artiklarna 13–14 GDPR, å andra sidan. Medan GDPR bygger på principen att den registrerade ska ha insyn i hur och varför personuppgifter behandlas, förutsätter penningtvättslagstiftningen i flera avseenden att behandlingen sker utan att kunden informeras. Denna normkollision aktualiserar grundläggande frågor om hur långtgående begränsningar av informationsrätten som kan accepteras i brottsbekämpningens namn.

Enligt GDPR ska den registrerade som huvudregel informeras om behandlingen av personuppgifter, inklusive dess ändamål, rättsliga grund och lagringstid. Principen om öppenhet är central för att individen ska kunna utöva sina rättigheter på ett effektivt sätt. AML-regelverket bryter emellertid med denna logik genom det så kallade tipping-off-förbudet, som innebär att verksamhetsutövaren inte får informera kunden om att denne övervakas, att en misstänkt transaktion har rapporterats eller att en utredning kan vara pågående.

Syftet är att kunden anpassar sitt förhindra att beteende, undanröjer bevis eller på annat sätt försvårar en pågående brottsutredning.

Rätten till information är dock inte absolut. Begränsningar kan följa av sektorsreglering och nationell rätt med stöd av artikel 23 GDPR, förutsatt att kraven på lagstöd, nödvändighet och proportionalitet är uppfyllda. I AML-sammanhang kommer detta till uttryck genom tipping-off-förbudet och tystnadsplikten, som syftar till att skydda rapporteringssystemets effektivitet och förhindra att misstänkta aktörer varnas. Den avgörande frågan är därför inte om informationsrätten kan begränsas, utan om den generella och långtgående sekretess som följer av AML-regelverket är nödvändig och proportionerlig i förhållande till syftet.

Konflikten blir särskilt tydlig i fintech-sektorn. Fintech-bolag och digitala banker profilerar sig ofta genom användarvänlighet, öppenhet och realtidsinformation. Kunderna förväntar sig omedelbar återkoppling, detaljerad insyn i transaktioner och tydlig kommunikation om vad som sker i deras konton och applikationer. Samtidigt kräver AML-regelverket att övervakning och rapportering sker diskret. För ett fintech-bolag innebär detta en inneboende spänning mellan att bygga förtroende genom öppenhet och att efterleva ett regelverk som i stor utsträckning bygger på tystnad gentemot kunden.

I praktiken innebär detta att kunden inte kan förstå varför en transaktion fördröjs eller varför ytterligare uppgifter begärs, samtidigt som kunden saknar möjlighet att bedöma eller angripa den underliggande personuppgiftsbehandlingen. Därmed uppstår en rättssäkerhetsdimension: begränsad insyn minskar den registrerades faktiska möjligheter att utöva rättigheter enligt GDPR.

Ur ett rättssäkerhetsperspektiv innebär detta att den registrerade i praktiken saknar möjlighet att kontrollera om behandlingen är korrekt, laglig och proportionerlig. När informationsasymmetrin är total försvagas de processuella garantier som annars utgör en central del av dataskyddsregimen, vilket riskerar att förskjuta balansen till fördel för effektivitet på bekostnad av rättighetsskydd.

För att bedöma om denna inskränkning är rättsligt försvarbar måste även denna konflikt prövas mot proportionalitetsprincipen i artikel 52.1 i EU-stadgan. Att begränsa informationsrätten kan i ett första led anses vara ägnat att skydda rapporteringssystemets effektivitet och att förhindra att misstänkta personer varnas. Nödvändighetsbedömningen är dock mer komplex. Sekretessundantaget tillämpas generellt och utan individuell prövning, oavsett kundens riskprofil eller graden av misstanke. Det kan därför ifrågasättas om ett mer nyanserat system –

exempelvis där information lämnas i efterhand eller i mer generella ordalag – skulle kunna uppnå samma syfte med ett mindre ingrepp i den registrerades rättigheter.

Vid proportionalitetsbedömningen i snäv mening måste även konsekvenserna för den enskilde beaktas. Eftersom kunden inte får informeras om övervakning eller rapportering saknas i praktiken möjligheten att utöva rättigheter såsom rättelse, begränsning eller invändning mot behandlingen. När detta kombineras med långvarig lagring av omfattande finansiella uppgifter förstärks integritetsintrånget. För fintech kunder, vars ekonomiska liv i hög grad är digitaliserat, innebär detta att mycket detaljerade beteendemönster behandlas och analyseras utan deras vetskap.

EU-domstolens praxis visar att även åtgärder som syftar till att skydda nationell säkerhet eller bekämpa brottslighet måste vara strikt nödvändiga och förenade med tillräckliga rättssäkerhetsgarantier.[71] Särskild vikt har lagts vid behovet av effektiva kontrollmekanismer och begränsningar i tillämpningen av generella övervakningsåtgärder. Även om AML-systemet skiljer sig från statlig massövervakning illustrerar rättspraxis att proportionalitetsbedömningen måste beakta intrångets omfattning samt vilka rättssäkerhetsgarantier som faktiskt står till den registrerades förfogande.[72]

Sammantaget framstår sekretessundantagen inom AML-regelverket som funktionellt motiverade men rättsligt problematiska i sin nuvarande utformning. Även om syftet att bekämpa penningtvätt och skydda det finansiella systemet är legitimt, väcker den generella och automatiska begränsningen av informationsrätten frågor om balansen mellan brottsbekämpning och personlig integritet är tillräckligt finjusterad. I en digital finansmarknad blir denna normkollision särskilt påtaglig.

Sammanfattningsvis kan sekretessreglerna motiveras av AML-systemets funktion, men deras generella karaktär innebär att proportionalitetsbedömningen blir särskilt krävande. Avsaknaden av individuell differentiering och efterhandsinformation försvagar rättssäkerhetsgarantierna och gör intrånget mer långtgående än vad som strikt nödvändigtvis krävs. Dessa två konfliktytor – lagring och sekretess – bildar tillsammans underlaget för den samlade proportionalitetsbedömning som genomförs nedan.

[71] EU-domstolen, *La Quadrature du Net*.

[72] EU-domstolen, *La Quadrature du Net*.

4.4 Ny AML-reglering och GDPR-konflikter

Som framgått i inledningen tar denna uppsats sin utgångspunkt i det nya europeiska AML-paketet, bestående av förordningen om åtgärder mot penningtvätt och finansiering av terrorism (AMLR), det sjätte penningtvättsdirektivet (AMLD6) samt inrättandet av den nya tillsynsmyndigheten AMLA. Paketet syftar till att stärka och harmonisera det penningtvättsförebyggande regelverket inom EU, bland annat genom mer enhetliga regler och en mer centraliserad tillsyn. Frågan är hur dessa reformer påverkar de konflikter mellan AML-regelverket och GDPR som har analyserats ovan, särskilt ur ett fintech-perspektiv.

En central förändring är att AMLR ges formen av en EU-förordning, vilket innebär att reglerna blir direkt tillämpliga och mer enhetliga i medlemsstaterna. För fintech-bolag som ofta verkar gränsöverskridande kan detta innebära ökad rättssäkerhet och förutsebarhet, eftersom skillnader i nationell implementering minskar. Samtidigt riskerar en mer detaljerad och bindande reglering att förstärka de redan identifierade konflikterna. När bevarandetider och kundkännedomsåtgärder fastställs på EU-nivå minskar utrymmet för nationella eller individuella anpassningar, exempelvis riskbaserade lagringsmodeller som bättre skulle kunna harmoniera med GDPR:s princip om lagringsminimering.

Även i fråga om öppenhet och informationsrätt kan det nya regelverket innebära en förskjutning. AMLD6 stärker kraven på rapportering och samarbete mellan myndigheter, vilket i praktiken kan leda till mer omfattande och kontinuerlig övervakning av kunder. För fintech-aktörer, vars affärsmodeller bygger på snabbhet och realtidsbaserad kommunikation med användaren, kan detta ytterligare fördjupa konflikten mellan tipping-off-förbudet och kundernas förväntningar på insyn. Även om regelverket tydliggör verksamhetsutövarens skyldigheter ger det begränsad vägledning om hur dessa ska balanseras mot dataskyddsrättsliga principer i praktiken.

Inrättandet av AMLA innebär samtidigt en potentiell förändring i hur dessa konflikter kan hanteras framöver. Genom en mer centraliserad tillsyn och samordning av nationella myndigheter finns en möjlighet till mer enhetliga tolkningar av AML-regelverket, även i relation till GDPR. För fintech-bolag kan detta innebära att osäkerheten kring hur långtgående databehandling och sekretessåtgärder får vara minskar. Samtidigt är det ännu oklart i vilken utsträckning AMLA kommer att beakta dataskyddsaspekter i sin tillsyn, eller hur samspelet med nationella dataskyddsmyndigheter kommer att fungera i praktiken.

Sammantaget talar reformen för att spänningarna behöver hanteras mer uttryckligt inom unionsrätten, antingen genom tydligare dataskyddsgarantier i AML-regleringen eller genom vägledning om hur proportionalitetskraven ska operationaliseras vid lagring och sekretess. Det är särskilt relevant för fintech-aktörer, där datavolymer och automatiserad övervakning förstärker intrångets omfattning.

4.5 Proportionalitetsbedömning av AML:s inskränkningar

De konflikter som har identifierats i föregående avsnitt – dels mellan bevarandekrav och lagringsminimering, dels mellan sekretess och rätten till information – aktualiserar frågan i vilken utsträckning AML-regelverkets inskränkningar i den registrerades rättigheter enligt GDPR är rättsligt försvarbara. För att besvara denna fråga krävs en samlad prövning mot proportionalitetsprincipen i artikel 52.1 i EU-stadgan, enligt vilken varje begränsning av grundläggande rättigheter ska vara föreskriven i lag, respektera rättighetens väsentliga innehåll samt vara nödvändig och proportionerlig i förhållande till ett legitimt mål av allmänt intresse. I denna prövning måste särskild vikt fästas vid om inskränkningarna respekterar rättigheternas väsentliga innehåll samt om det finns tillräckliga rättssäkerhetsgarantier, såsom kontrollmekanismer, begränsningar i åtkomst och möjlighet till efterhandsprövning. Avsaknad av sådana garantier kan medföra att en åtgärd, trots legitimt syfte, inte uppfyller proportionalitetskravet enligt unionsrätten.

Det står klart att de aktuella begränsningarna är föreskrivna i lag och syftar till ett legitimt mål, nämligen att förebygga och bekämpa penningtvätt och finansiering av terrorism samt att skydda det finansiella systemets integritet. Proportionalitetsfrågan gäller därför inte om syftet i sig är godtagbart, utan om de medel som används för att uppnå detta syfte är rimligt avvägda i förhållande till den enskildes rätt till skydd för personuppgifter och privatliv.

Vid en samlad proportionalitetsbedömning framträder två genomgående problem. För det första är flera inskränkningar generellt utformade och träffar även lågriskkunder, vilket försvagar nödvändighetsargumentet. För det andra är de processuella garantierna för den registrerade begränsade i de situationer där insyn utesluts, vilket gör att intrånget i praktiken kan bli mer långtgående än vad lagstiftaren avsett. Sammantaget talar detta för att regleringens legitima syfte inte är ifrågasatt, men att proportionaliteten i utformning och tillämpning är det mest problematiska ledet, särskilt i en digital och datadriven miljö.

Den samlade proportionalitetsbedömningen visar att AML-regelverkets inskränkningar i dataskyddet i grunden är legitima och motiverade av ett betydande allmänintresse. Samtidigt framgår att den generella och odifferentierade utformningen av lagrings- och sekretessregler riskerar att gå längre än vad som är strikt nödvändigt i enskilda fall, särskilt i förhållande till lågriskkunder och i datadrivna digitala miljöer. Konflikten ligger därmed inte i regelverkens legitimitet, utan i hur finjusterat de tillämpas. Detta talar för ett behov av mer differentierade lösningar och tydligare rättssäkerhetsgarantier, där effektiv brottsbekämpning förenas med ett reellt skydd för den personliga integriteten.

5 Slutsatser: En avvägning mellan brottsbekämpning och personlig integritet

Analysen i denna uppsats har visat att relationen mellan AML-regelverket och GDPR inte präglas av en direkt normkonflikt, utan av en mer grundläggande strukturell spänning mellan två legitima och unionsrättsligt erkända intressen: behovet av effektiv brottsbekämpning och skyddet för den enskildes personliga integritet. Denna spänning är inte ny, men får ett tydligare genomslag i en digitaliserad finans-marknad där omfattande databehandling utgör en integrerad del av verksamheten, särskilt inom fintech-sektorn.

När det gäller frågan om lagring av kunduppgifter visar analysen att den femåriga bevarandetiden enligt penningtvättsregelverket i grunden kan rymmas inom GDPR:s systematik, eftersom behandlingen vilar på en rättslig förpliktelse och därmed begränsar rätten till radering enligt artikel 17.3 b GDPR. Detta innebär dock inte att varje tillämpning automatiskt uppfyller unionsrättens krav. Den generella och odifferentierade utformningen innebär att även lågriskkunder omfattas av långtgående lagring oberoende av konkret risk eller misstanke. I en digital miljö, där mängden insamlade uppgifter är betydligt större än i traditionell bankverksamhet, kan intrångets faktiska omfattning bli mer ingripande. Lagringsregeln framstår således som rättsligt möjlig, men dess proportionalitet är i praktiken beroende av hur nödvändighetskravet tolkas och tillämpas.

En motsvarande spänning framträder i fråga om rätten till information. Begränsningar av informationsrätten kan motiveras av AML-systemets funktion, särskilt för att undvika tipping-off och skydda brottsutredningar, och har stöd i artikel 23 GDPR i kombination med nationella regler om tystnadsplikt. Samtidigt innebär den generella sekretess som följer av regelverket att den registrerade i praktiken får begränsade möjligheter att förstå, kontrollera och påverka behandlingen av sina personuppgifter. När öppenhet kombineras med långvarig lagring förstärks integritetsintrångets betydelse, särskilt i digitala och datadrivna miljöer där behandlingen är omfattande och ofta automatiserad.

Den samlade proportionalitetsbedömningen enligt artikel 52.1 i EU-stadgan visar att AML-regelverkets inskränkningar i dataskyddet syftar till ett legitimt och tungt vägande allmänintresse.

Problemet ligger inte i målets godtagbarhet, utan i åtgärdernas generella och enhetliga utformning. Fasta lagringstider och omfattande sekretessregler tillämpas i stor utsträckning utan tydlig differentiering utifrån risk, teknik eller verksamhetsmodell, vilket riskerar att göra regleringen relativt trubbig i en rättsordning som i övrigt bygger på proportionalitet och riskbaserade bedömningar.

Sammantaget visar uppsatsen att AML-regelverket och GDPR i grunden är förenliga inom unionsrättens ram, men att balansen mellan effektiv brottsbekämpning och skyddet för den personliga integriteten i hög grad avgörs av hur reglerna tilllämpas i praktiken. I en digitaliserad finansmarknad, där datamängderna är omfattande och behandlingen ofta automatiserad, skärps kraven på en mer nyanserad och finjusterad tillämpning. En rättsligt hållbar balans förutsätter därför inte en omprövning av regelverkens legitimitet, utan en utveckling mot mer differentierade lösningar och tydligare rättssäkerhetsgarantier, där dataskyddet ges reell betydelse samtidigt som AML-systemets brottsförebyggande funktion upprätthålls.

Källförteckning

Offentligt tryck

EU-rättsligt material

Fördrag och stadgor

Europeiska unionens stadga om de grundläggande rättigheterna (2012/C 326/01).

Förordningar

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).

Europaparlamentets och rådets förordning (EU) 2024/1620 av den 31 maj 2024 om inrättande av en myndighet för bekämpning av penningtvätt och finansiering av terrorism (AMLA-förordningen).

Europaparlamentets och rådets förordning (EU) 2024/1624 av den 31 maj 2024 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism (AMLR).

Direktiv

Europaparlamentets och rådets direktiv 2001/97/EG av den 4 december 2001 om ändring av rådets direktiv 91/308/EEG om åtgärder för att förhindra att det finansiella systemet används för tvättning av pengar (2AMLD).

Europaparlamentets och rådets direktiv 2005/60/EG av den 26 oktober 2005 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt och finansiering av terrorism (3AMLD).

Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism [...] (4AMLD).

Europaparlamentets och rådets direktiv (EU) 2018/843 av den 30 maj 2018 om ändring av direktiv (EU) 2015/849 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism (5AMLD).

Europaparlamentets och rådets direktiv (EU) 2018/1673 av den 23 oktober 2018 om bekämpande av penningtvätt genom straffrättsliga medel (straffrättsliga penningtvättsdirektivet).

Europaparlamentets och rådets direktiv (EU) 2024/1640 av den 31 maj 2024 om de mekanismer som medlemsstater ska inrätta för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism (6AMLD).

Förslag och soft law

Europeiska dataskyddsstyrelsen (EDPB), Guidelines 01/2022 on data subject rights – Right of access.

Europeiska dataskyddsstyrelsen (EDPB), Guidelines on Transparency under Regulation 2016/679.

Europeiska dataskyddsstyrelsen (EDPB), Guidelines on Article 23 GDPR.

Europeiska kommissionen, Commission Staff Working Document – Supranational Risk Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Union, SWD(2019) 650 final.

Europeiska kommissionen, Förslag till Europaparlamentets och rådets förordning om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, COM(2021) 420 final.

Svenskt offentligt tryck

Propositioner

Prop. 2003/04:156, Gäldenärsbrott och brott mot borgenärer m.m.

Prop. 2016/17:173, En effektivare bekämpning av penningtvätt.

Prop. 2017/18:105, Ny dataskyddslag.

Prop. 2017/18:216, En ny penningtvättslag..

Statens offentliga utredningar (SOU)

SOU 2016:8, Ytterligare åtgärder mot penningtvätt och finansiering av terrorism.

SOU 2022:58, Skärpta regler om kundkännedom.

SOU 2024:58, En ny lag om åtgärder mot penningtvätt och finansiering av terrorism.

Lagar och författningar

Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism.

Rättsfall

EU-domstolen

C-617/10, Åklagaren mot Hans Åkerberg Fransson, EU:C:2013:105.

C-293/12 och C-594/12, Digital Rights Ireland Ltd mot Minister for Communications, Marine and Natural Resources m.fl., EU:C:2014:238.

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

C-362/14, Maximillian Schrems mot Data Protection Commissioner, EU:C:2015:650.

C-203/15 och C-698/15, Tele2 Sverige AB mot Post- och telestyrelsen m.fl., EU:C:2016:970.

C-311/18, Data Protection Commissioner mot Facebook Ireland Ltd och Maximillian Schrems (Schrems II), EU:C:2020:559.

C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., EU:C:2020:791.

Litteratur

Bernitz, Ulf (red.), EU:s stadga om de grundläggande rättigheterna: En kommentar, Norstedts Juridik, Stockholm 2021.

Bernitz, Ulf, Heuman, Lars, Leijonhufvud, Madeleine, Seipel, Peter, Warnling Conradsson, Wiweka & Vogel, Hans-Heinrich, Finna rätt – juridikens källmaterial och arbetsmetoder, 16 uppl., Norstedts Juridik, Stockholm 2023.

Bygrave, Lee A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, Haag 2002/2014.

Kleineman, Jan, ”Rättsdogmatisk metod”, i Nääv, Maria & Zamboni, Mauro (red.), Juridisk metodlära, 2 uppl., Studentlitteratur, Lund 2018.

Kuner, Christopher, Transborder Data Flows and Data Privacy Law, Oxford University Press, Oxford 2013.

Kuner, Christopher, Bygrave, Lee A. & Docksey, Christopher (red.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford 2020.

Peczenik, Aleksander, Juridikens teori och metod: en introduktion till allmän rättslära, Fritze, Stockholm 1995.

Van der Sloot, Bart, Privacy as Virtue: Moving Beyond the Individual in the Age of Big Data, Intersentia, Cambridge 2017/2018.

Zetterquist, Ola, ”EU-rättslig metod”, i Dahlman, Christian & Wahlberg, Lena (red.), Juridiska grundbegrepp: En vänbok till David Reidhav, Studentlitteratur, Lund 2019.

Internetkällor

Financial Action Task Force (FATF), The 40 Recommendations, 1990 (med senare uppdateringar).

Financial Stability Board (FSB), Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits, 2017.

Finansinspektionen, Erfarenheter från penningtvättsrapporteringen, elektronisk rapport, 2024.

Finansinspektionen, Riskbaserat förhållningssätt och kundkännedom, vägledning, 2022-09-20.

Integritetsskyddsmyndigheten (IMY), Personuppgifter i penningtvättsrapporteringen – sekretess och GDPR, 2022.

Integritetsskyddsmyndigheten (IMY), GDPR – Syfte och tillämplighet, [hämtad 2026].

Integritetsskyddsmyndigheten (IMY), Vägledning om GDPR och brottsbekämpning, [hämtad 2026].