LUNDS UNIVERSITET
EKONOMI-
HÖGSKOLAN

Öppen finans och dataskyddsrätt

Samspelet mellan den föreslagna ramförordningen om öppna finansiella tjänster och EU:s dataskyddsbestämmelser

Layal Sibai

INSTITUTIONEN FÖR HANDELSRÄTT

Affärsjuridisk kandidatuppsats

15 högskolepoäng

HARH13

VT 2024

Sammanfattning

Syftet med denna uppsats är att undersöka samspelet mellan den föreslagna förordningen om öppen finans (FiDA) från 2023 och EU:s dataskyddsbestämmelser, särskilt dataskyddsförordningen (GDPR). Enligt EU-kommissionens strategi för digital finans från 2020 är främjandet av datadriven finansiering en prioritet. I takt med att mängden data och digital teknikens påverkan på ekonomin ökar, blir det allt viktigare att skapa en säker ram för datadelning som skyddar kundernas personliga integritet och samtidigt främjar innovation och konkurrens inom den finansiella sektorn.

Trots att GDPR har etablerat rätten till dataportabilitet, har denna rättighet haft begränsad praktisk tillämpning, särskilt inom finansiella tjänster. Bristande incitament för finansiella institutioner, osäkerhet och låg tillit hos de registrerade samt avsaknad av tekniska gränssnitt och standardisering har försvårat användningen av denna rättighet.

Uppsatsen fokuserar på tre huvudsakliga frågeställningar: Vilka skyldigheter har personuppgiftsansvariga att göra kunddata inom finansiella tjänster tillgänglig för dataanvändare enligt EU:s dataskyddsbestämmelser, särskilt rätten till dataportabilitet? Vilka skyldigheter har personuppgiftsansvariga enligt den föreslagna förordningen? Hur samspelar den föreslagna ramförordningen med de befintliga dataskyddsbestämmelserna med avseende på dataportabilitet?

FiDA bygger till stor del på GDPR och kräver att alla skyldigheter i artiklarna 5, 6 och 9 i GDPR efterlevs när data delas och hanteras. Under GDPR måste personuppgiftsansvariga säkerställa säker överföring av personuppgifter och interoperabilitet i de tekniska formaten. Vidare är personuppgiftsansvariga även skyldiga att informera individer om deras rättigheter avseende dataportabilitet, men dessa skyldigheter gäller endast om överföringen är tekniskt möjlig. Å andra sida ålägger FiDA datainnehavare att på begäran tillhandahålla kunddata till dataanvändare på ett säkert och standardiserat sätt. FiDA inför också specifika skyldigheter för dataanvändare att hantera och använda kunddata enligt fastställda regler, samt att erbjuda ett tekniskt system för tillståndshantering.

Ämnesord: Öppen finans, Financial Data Access (FiDA), dataskyddsförordning (GDPR), Dataportabilitet,

Abstract

The purpose of this thesis is to examine the interaction between the proposed Financial Data Access (FiDA) regulation from 2023 and the EU's data protection regulations, particularly the General Data Protection regulation (GDPR). According to the EU Commission's digital finance strategy from 2020, promoting data-driven finance is a priority. As the amount of data and the impact of digital technology on the economy increase, it becomes increasingly important to establish a secure framework for data sharing that protects customer privacy while promoting innovation and competition in the financial sector.

Despite GDPR establishing the right to data portability, this right has seen limited practical application, especially within financial services. The lack of incentives for financial institutions, uncertainty and low trust among data subjects, and the absence of technical interfaces and standardization have hindered the use of this right.

The thesis focuses on three main questions: What obligations do controllers have to make customer data available to data users in financial services according to EU data protection regulations, particularly regarding the right to data portability? What obligations do controllers have under the proposed regulation? How does the proposed framework regulation interact with existing data protection regulations regarding data portability?

FiDA heavily builds on GDPR and requires compliance with all obligations set out in Articles 5, 6, and 9 of GDPR when sharing and handling data. Under GDPR, data controllers must ensure the secure transfer of personal data and interoperability of technical formats. Controllers are also obliged to inform individuals about their data portability rights, but these obligations may only apply if the transfer is technically feasible. On the other hand, FiDA mandates data holders to provide customer data to data users on request in a secure and standardized manner. It also imposes specific obligations on data users to manage and use customer data according to established rules, including providing a technical system for managing permissions.

Keywords: Open finance, Financial Data Access (FiDA), General Data Protection Regulation (GDPR),, Data portability.

Förord

Ett varmt tack riktas till min handledare, Jonas Ledendal, vars ovärderliga vägledning och stöd har varit avgörande för denna uppsats. Hans insikter och råd har inte bara förbättrat kvaliteten på arbetet utan också gjort skrivprocessen mycket smidigare och mer givande. Tack vare hans expertis och engagemang har jag kunnat utveckla mina idéer och fördjupa min förståelse inom ämnet på ett sätt som jag tidigare inte trodde var möjligt.

Jag vill även uttrycka min djupaste tacksamhet till min familj, som ständigt har funnits där för att uppmuntra och inspirera mig. Ett särskilt tack går till min bror, vars råd och uppmuntran har varit ovärderliga under hela denna resa. Hans stöd har gett mig styrka och motivation när jag har behövt det som mest.

Att ha nått denna punkt i mitt arbete är inte bara resultatet av några månaders arbete, utan resultat av en resa som började för sju år sedan när jag flyttade till Sverige. Det är en prestation som jag en gång trodde var omöjlig.

Slutligen vill jag rikta ett stort tack till dig som nu ska läsa denna uppsats. Jag hoppas att du finner den både intressant och givande. Det har varit en lärorik och utvecklande resa för mig att skriva denna uppsats, och jag önskar dig mycket nöje i läsningen.

Layal Sibai
Lund den 2 juni 2024

Innehåll

Förkortningar

Artikel 29-arbetsgruppen	Formellt arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter. Den är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet
EDPB	European Data protection Board, (Europeiska dataskyddsstyrelsen)
EDPS	European Data Protection Supervisor, (Europeiska datatillsynsmannen)
CJEU	Court of Justice of the European Union
EU	Europeiska unionen
FiDA	Förslag till europaparlamentets och rådets förordning om en ram för åtkomst till finansdata och om ändring av förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010, (EU) nr 1095/2010 och (EU) 2022/2554
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
PSD2	Betaltjänstdirektivet (EU) 2015/2366

1 Inledning

1.1 Bakgrund

Mängden data som genereras runt om i världen ökar i en rasande takt och den digitala tekniken har under de senaste åren omvälvt ekonomin och samhället i sin helhet genom dess påverkan på alla verksamhetsområden. År 2020 antog Europeiska kommissionen en strategi för att främja tillväxten av dataekonomin och skapa ett enhetligt europeiskt dataområde, öppet för världen, där data lagras, bearbetas och utnyttjas på ett säkert och innovativt sätt.[1] Jämfört med andra branscher är finanstjänster den största användaren av data i EU och företag inom finanssektorn som drivs av data har mycket att vinna på ökad datadelning.[2] EU:s datalagstiftning inom finanssektorn är en del av en större plan som syftar till att göra EU till en ledande dataekonomi. Genom att kräva att finansinstitut delar data om produkter, transaktioner och ekonomisk information, främjar EU inte bara transparens utan också digitalisering inom sektorn. Denna rörelse mot en omfattande användning av data har potential att öka ekonomisk effektivitet och underlätta hållbar utveckling.[3] Detta visar tydligt att data utgör en av de mest värdefulla tillgångarna för både myndigheter och privata företag, särskilt när det gäller personuppgifter.[4]

I en värld där data samlas in och används i stor skala, har skyddet av personuppgifter och den personliga integriteten dock blivit mer angeläget än någonsin. Detta är speciellt relevant inom finanssektorn, där finansinstitut i hög grad förlitar sig på kunddata för att tillhandahålla tjänster och utveckla produkter.[5] Dataskyddsförordningens (GDPR) centrala roll i detta sammanhang ger upphov till många frågor i samband med datahantering och datadelning. Med tanke på finansinstitutens beroende av att dela personuppgifter, är det av yttersta vikt att sådana uppgifter skyddas för att bevara kundförtroende.

Kunder bör ha rätt att bestämma över sina finansiella data och kunna ge företag åtkomst till dessa data för att ta del av finansiella tjänster och informationstjänster om de så önskar. Detta utgör vad som kallas för Öppen finans, vilket avser tillgång till och behandling av data mellan företag samt mellan företag och kunder enligt kundens begäran inom ett brett spektrum av finansiella tjänster. Detta exkluderar dock betalkontodata, som specifikt regleras av det andra betaltjänstdirektivet (PSD2) och betecknas som öppen banking, vilket enbart avser betalningstjänster.[6] För

[1] Meddelande från kommissionen till europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén, en EU-strategi för data, COM (2020) 66 final., s. 1.

[2] Commission Staff Working Document, Impact Assessment Report, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, SWD (2023) 224 final, s. 7.

[3] Ibid, s. 32.

[4] Ibid, s. 1.

[5] COM (2020) 66 final, En EU-strategi för data, s. 32.

[6] SWD (2023) 224 final, s. 6.

närvarande har kunder inom EU:s finansiella sektor, bortsett från betaltjänster som regleras av PSD2, ingen verklig kontroll över vem som har tillgång till deras data eller hur dessa data används.

Även om öppen banking och öppen finans omfattar olika verksamhetsområden har EU:s framgångsrika reglering av betaltjänster lagt en stabil grund för hur öppen finans kan regleras. Detta är särskilt relevant i förhållande till GDPR. Europeiska dataskyddsstyrelsen (EDPB) har formulerat riktlinjer angående interaktionen mellan PSD2 och GDPR. PSD2 inför nya bestämmelser för att säkerställa rättssäkerhet för konsumenter, näringsidkare och företag inom betalningskedjan. Detta direktiv skapar en rättslig ram för nya betaltjänstleverantörer att få tillgång till kunders betalkonton för att erbjuda dessa tjänster. Å andra sidan fastställer GDPR en grundläggande uppsättning standarder för företag som behandlar personuppgifter, vilket syftar till att förbättra skyddet av sådana uppgifter under behandling och överföring. Denna koppling har ökat intresset för vidareutveckling av regelverket för delning av annan kunddata än betalkontouppgifter inom finanssektorn.[7]

Europeiska kommissionen har lagt fram förslag som syftar till att skapa ett ramverk för öppna finansiella tjänster, i linje med målen som anges i EU:s strategi för digitalisering av finanssektorn. Det föreslagna ramverket, även känt som FiDA, är avsett att utformas som en förordning för öppna finansiella tjänster. FiDA är en ny lagstiftning och inte en ändring av tidigare EU-regler vilket innebär att det anses förenligt med både GDPR och PSD2, och utöver denna förenlighet har det också en stark överensstämmelse med Data Act[8] och Data Governance Act[9]. Innebörden av öppen finans är att en tredjepartsleverantör ges möjlighet att få tillgång till kundens finansiella information genom olika tekniska åtkomstmetoder. Med andra ord syftar FiDA till att lösa problem relaterade till kundernas tillgång till sin egna data genom att ge dessa ökad kontroll över vilka som får tillgång till deras finansiella information. På så sätt skulle kunderna erhålla tillgång till finansiella produkter och tjänster som är anpassade efter deras behov utifrån data som är relevanta för dem. Om detta uppnås kan förslaget leda till förbättrade ekonomiska utfall för användare av finansiella tjänster och på bredare skala även bidra till att utveckla en attraktiv dataekonomi inom EU.[10]

Att reglera åtkomst till kunddata betyder att främja teknisk och regleringsmässig interoperabilitet för dataåtkomst och infrastrukturer för data. Trots att GDPR framgångsrikt har reglerat hanteringen av personuppgifter, tyder det på att det fortfarande finns begränsningar när det gäller att dela information med tredje parter på ett effektivt sätt. Möjligheten för tredjepartstjänsteleverantörer att agera som dataanvändare och få tillgång till data baserat på kundens begäran enligt rätten till dataportabilitet enligt artikel 20 i GDPR kan vara svår att utöva i praktiken. Rätten för registrerade att flytta data innebär inte uttryckligen att de kan göra det kontinuerligt eller i realtid.[11] FiDA tillämpas på både datainnehavare och

[7] EDPB, riktlinjer 06/2020 om samspelet mellan andra betaltjänstdirektivet och dataskyddsförordningen, version 2.0, s. 2–3.

[8] Se 2020/1828.

[9] Se 2022/868.

[10] Proposal for a regulation of the European parliament and of the council on a framework for Financial Data Access and amending Regulations (EU), COM (2023) 360 final, 2023/0205 (COD), s. 2.

[11] SWD (2023) 224 final, s. 17.

dataanvändare. Bland dataanvändarna finns kreditinstitut, försäkringsbolag, värdepappersbolag och andra finansiella företag. Dessutom anses leverantörer av finansiell information som dataanvändare. Således kommer FiDA, med initiativet för öppen finans, att kunna anpassa sig bättre till den datadrivna ekonomin inom sektorn.

1.2 Syfte och frågeställningar

Syftet med den här uppsatsen är att undersöka de skyldigheter som åläggs personuppgiftsansvariga enligt den förslagna ramförordningen för åtkomst till kunddata inom finansiella tjänster samt skyldigheterna om dataportabilitet som redan gäller enligt EU:s dataskyddsbestämmelser. Uppsatsens övergripande syfte kommer att studeras utifrån följande frågeställningar:

- Vilka skyldigheter har personuppgiftsansvariga att göra kunddata inom finansiella tjänster tillgänglig för dataanvändare enligt EU:s dataskyddsbestämmelser, särskilt rätten till dataportabilitet?

- Vilka skyldigheter har personuppgiftsansvariga vid att göra kunddata inom finansiella tjänster tillgängliga enligt den föreslagna förordningen?

- Hur samspelar den föreslagna ramförordningen med de befintliga dataskyddsbestämmelserna med avseende på dataportabilitet?

1.3 Avgränsningar

Denna uppsats innehåller tre huvudsakliga avgränsningar, vilket är nödvändigt med tanke på det breda område som de behandlade regelverken beaktar.

Den första avgränsningen fokuserar på det nya förslaget till ramförordning, särskilt dess relation till PSD2. Även om det kan bli nödvändigt att referera till PSD2 för att klargöra vissa termer eller etablerad praxis, kommer denna uppsats inte erbjuda en grundlig analys av betalningstjnster eller öppen banking i sig.

Den andra avgränsning gäller dataskyddsbestämmelserna. Analysen kommer primärt att undersöka dataskyddsrättsliga frågor utifrån syftet och frågeställningen med uppsatsen. Även om annan lagstiftning såsom Data Governance Act, Data Act och PSD2 kan komma att omnämnas, kommer detta endast att ske där det finns särskilda skäl som motiverar deras relevans. Detta val av avgränsning möjliggör en djupgående analys av de centrala juridiska frågorna men begränsar samtidigt perspektivet genom att inte beakta förhållandet till andra unionsrättsliga regelverk.

Den tredje avgränsningen görs med hänsyn till tolkningen och tillämpningen av vissa begrepp och bestämmelser inom GDPR. Analysen kommer inte att omfatta personuppgiftsbiträdenas roll, utan i stället fokusera på personuppgiftsansvariga och deras ansvar vid hanteringen av finansiella data enligt det föreslagna ramverket. Vidare kommer inte samtliga rättsliga grunder att behandlas, utan uppsatsen kommer att koncentrera sig på de rättsliga grunderna samtycke, avtals ingående och fullgörande samt intresseavvägning, eftersom dessa är särskilt relevanta för åtkomst till och hantering av finansiella data.

1.4 Metod och material

Vald metod avgör vilket material som är aktuellt att undersöka närmare.[12] Rättsdogmatisk metod kommer att används som en huvudmetod med syfte att göra en analys av gällande rätt. Rättsdogmatisk metod syftar till att tolka och tillämpa rättsregler genom en systematisk analys av tillgängliga rättskällor såsom lagstiftning, rättspraxis och juridisk litteratur. Metoden fokuserar på att rekonstruera en rättsregel eller lösningen på ett rättsligt problem genom att tillämpa en rättsregel på det aktuella problemet.[13] Genom en djupgående undersökning av olika rättskällor, inklusive lagar och rättspraxis, strävar metoden efter att tydligt redogöra för hur en rättsregel bör tolkas och tillämpas i praktiken. Rättsdogmatiken betonar även vikten av att korrekt identifiera och formulera rättsliga frågeställningar och att noggrant analysera och argumentera för en specifik lösning.[14]

Eftersom den här uppsatsen fokuserar på EU-rätt kommer undersökningen att även använda den EU-rättsliga metoden, en anpassad form av rättsdogmatisk metod som är särskilt utformad för att hantera EU-rättsliga källor. EU utgör en tydligt överstatlig organisation med unika egenskaper, vilket avspeglas i dess rättssystem och den tillhörande juridiska metoden.[15] Denna metod omfattar inslag som har sina rötter i internationell rätt, men också element som normalt återfinns i nationella rättssystem.[16] Vidare anses teleologisk tolkning ha en framträdande roll, vilket innebär att den är inriktad på lagstiftningens ändamål. Detta betonar att rättsliga bestämmelser inte bör tolkas isolerat, utan i ljuset av deras sammanhang och syften.[17]

EU-rätten har utvecklat ett omfattande regelverk som skapar en normhierarki, vilken kontinuerligt utvecklas genom ny lagstiftning och rättspraxis från Europeiska unionens domstol (EU-domstolen). Denna hierarki grundar sig på en fundamental indelning i primärrätt och sekundärrätt. Vidare delas denna in i bindande och vägledande rättskällor.[18] De bindande rättskällorna inkluderar primärrätten, såsom fördragen och rättighetsstadgan, samt bindande sekundärrätt, internationella avtal, allmänna rättsprinciper. samt och EU-domstolens praxis. Vad som utgör vägledande rättskällor är icke bindande sekundärrätt, förarbeten, generaladvokaternas förslag till avgöranden, den EU-rättslig doktrinen samt ekonomiska teorier.[19] Det kan konstateras att primärrätten således utgör den grundläggande ram som sekundärrätten bygger på.

När det gäller material som ska används för att besvara uppsatsens frågeställningar utgår en del av uppsats från dataskyddsförordningen, vilken betraktas som en bindande och i medlemsstaterna direkt tillämplig rättskälla enligt den EU-rättsliga metoden. Uppsatsen hänvisar till en stor mängd andra bindande källor såsom

[12] Elsa Trolle Önnerfors och Henrik Wenander, att skriva rätt: Goda rad för att skriva uppsats i juridik, upplaga 3, 2022, s. 20.

[13] Jan Kleineman, Rättsdogmatiskmetod, upplaga 2, 2018 s. 21.

[14] Ibid, s. 35.

[15] Ulf Bernitz, Finna rätt, Juristens källmaterial och arbetsmetoder, upplaga 16 s. 63.

[16] Jane Reichel, EU-rättslig metod, upplaga 2, 2018, s. 110.

[17] Jörgen Hettne, EU-rättslig metod, upplaga 2, 2011, s. 34.

[18] Bernitz, s. 67.

[19] Hettne, s. 109.

PSD2[20], Data Act[21], Data Governance Act[22] och förordning om en ram för det fria flödet av andra data än personuppgifter i EU[23]. Uppsatsen tar även upp ett antal icke-bindande rättskällor inom sekundärrätten, inklusive förarbeten, riktlinjer, yttranden och rekommendationer från både EDPB och Europeiska kommissionen, samt från Artikel 29-arbetsgruppen. Det är viktigt att notera att Artikel 29-arbetsgruppen, som inrättades genom direktiv 95/46/EG, har ersatts av EDPB. Därför används arbetsgruppens yttranden enbart när EDPB inte har utfärdat någon relevant riktlinje eller yttrande. Detta är väsentligt att understryka eftersom EDPB har tagit över den rollen från Artikel 29-gruppen. Vidare kommer relevant rättsvetenskaplig litteratur också att användas. Dessa icke-bindande källor spelar en viktig roll i tolkningen av de bindande rättskällorna.

Den andra delen av uppsatsen behandlar den föreslagna ramförordningen, som betraktas som en icke-bindande rättskälla. Denna förordning, som presenterats av EU-kommissionen, har ännu inte blivit en del av den gällande EU-rätten och medför därför olika utmaningar, särskilt med hänsyn till bristen på rättspraxis. För att grundligt undersöka detta förslag har jag valt att analysera det utifrån själva förslaget och dess förarbeten, samt tillhörande riktlinjer, yttranden och doktrin. Eftersom den föreslagna ramförordningen grundar sig på ett antal regelverk, kommer analysen av vissa delar av förordningen att stödjas på dessa dokument. Genom att undersöka dessa aspekter kan uppsatsen bidra till en djupare förståelse för förslaget.

1.5 Disposition

Förutom det första kapitlet delas uppsatsen upp i tre huvuddelar. Uppdelningen har gjorts i enlighet med frågeställningarna för att underlätta för läsaren att följa med. I det första kapitlet presenteras en omfattande bakgrund till uppsatsens ämne, dess syfte och frågeställningar, avgränsningar samt den metod och det material som används i uppsatsen.

Det andra kapitlet som rör GDPR, och behandlar särskilt personuppgiftsansvarigas skyldigheter och rätten till dataportabilitet, är indelat i fyra huvuddelar. Kapitlet börjar med en översiktlig introduktion i avsnitt 2.1. Därefter följer avsnitt 2.2 som behandlar tre nyckelbegrepp som tydliggör tolknings- och tillämpningsområdet för regelverket. Avsnitt 2.3 behandlar principen om laglighet i artikel 5 GDPR. I detta avsnitt fördjupas diskussionen om laglighetsprincipen, de rättsliga grunderna för behandling av personuppgifter och reglerna för behandling av särskilda kategorier av personuppgifter. Dessa avsnitt lägger en grund för att undersöka rätten till dataportabilitetsbestämmelsen i avsnitt 2.4. Dessa avsnitt utgör en grund för att undersöka rätten till dataportabilitet i avsnitt 2.4. Detta avsnitt är ytterligare uppdelat i tre delar: avsnitt 2.4.1 behandlar principer och dataportabilitets, 2.4.2 fokuserar på samtycke som rättslig grund, och 2.4.3 diskuterar avtalets ingående och fullgörande som rättslig grund. Avsnitt 2.5 tar upp bestämmelserna om behandling av särskilda

[20] Se 2015/2366.
[21] Se 2020/1828.
[22] Se 2022/868.
[23] Se 2018/1807.

kategorier av personuppgifter. Slutligen avslutas kapitlet med en sammanfattning i avsnitt 2.6.

Det tredje kapitel behandlar särskilt tillgängliggörandet av kunddata enligt den föreslagna ramförordningen. Kapitlet börjar med en översiktlig introduktion av regelverket i avsnitt 3.2, följt av en detaljerad förklaring av de grundläggande begreppen, vilket tydliggör tolknings- och tillämpningsområdet för förslaget i avsnitt 3.3. De första delarna är sammankopplade med avsnitt 3.4, där en beskrivning till FiDA:s bestämmelserna presenteras. Avslutningsvis sammanfattas huvudpunkterna för att säkerställa en konsekvent genomgång och förståelse av materialet.

Det sista kapitlet syftar till att besvara uppsatsens syfte och de identifierade frågeställningarna genom en slutsats och omfattande analys.

2 Personuppgiftsansvarigs skyldigheter och rätten till dataportabilitet enligt GDPR

2.1 Inledning

Inom EU är rätten till skydd av personuppgifter en grundläggande rättighet. Med den ökande användningen av datadrivna teknologier har en mängd dataskyddsbestämmelser utvecklats. Bland dessa regelverk är GDPR en central rättsakt. Syftet med GDPR är att skapa en enhetlig och hög skyddsnivå för fysiska personer samt att eliminera barriärer för det fria flöden av personuppgifter inom unionen.[24]

Detta kapitel tar sikte på GDPR och de relevanta bestämmelserna som syftar till att reglera skyddet av personuppgifter, särskilt i förhållande till rätten till dataportabilitet. Detta är för att besvara frågan om de personuppgiftsansvarigas skyldigheter att göra kunddata inom finansiella tjänster tillgängliga. Kapitlet är indelat i tre huvudavsnitt. Det inleds med en genomgång av särskilda begrepp för att etablera en gemensam förståelse i avsnitt 2.2. Begreppen som behandlas är bland annat personuppgifter, den registrerade, personuppgiftsansvarig. I avsnitt 2.3 behandlas principen om laglighet för själva behandlingsprocessen artikel 5 GDPR. Avsnitt 2.4 fokuserar på den registrerades rätt till dataportabilitet, vilken innebär en rätt att begära ut eller överföra personuppgifter som individen själv har tillhandahållit till den personuppgiftsansvarige. Detta avsnitt är indelat i tre delar. Delarna behandlar principerna och tillämpningsområdena för dataportabilitet samt de rättsliga grunderna för behandling (artikel 6 GDPR), med särskilt fokus på samtycke och fullgörande av avtal. Till sist tar avsnitt 2.5 hänsyn till bestämmelserna om särskilda kategorier av personuppgifter som regleras i artikel 9 GDPR.

2.2 Särskilda begrepp

2.2.1 Personuppgifter

Personuppgifter innefattar all typ av information som direkt eller indirekt kan kopplas till en levande fysisk person. Även krypterad eller kodad information kan betraktas som personuppgifter om det finns en nyckel som möjliggör att de kan kopplas till en specifik individ. Definitionen återges i artikel 4.1 GDPR, som lyder:

> "Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för

[24] Skäl 10 GDPR.

den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”

Artikeln tar sikte på de grundläggande principerna inom EU-rätten om fri rörlighet och rättigheterna för fysiska personer, särskilt rätten till privatliv.[25] Definitionen utgår från fyra beståndsdelar som är nära sammankopplade och beroende av varandra. Begreppet ”varje upplysning” visar tydligt lagstiftarens avsikt att skapa en omfattande och bred definition av personuppgifter. Den tar sikte på både objektiva och subjektiva upplysningar, åsikter och även bedömningar. Banksektorn är ett typiskt exempel på den sistnämnda typen där bedömningar ofta görs av låntagarens pålitlighet, liksom inom försäkringsbranschen och i arbetsrelaterade situationer. Det måste konstateras att en upplysning inte behöver vara sann eller bekräftad för att utgöra en ”personuppgift”. Uppgifternas format spelar ingen roll då allt som finns tillgängligt i form av text, siffror, diagram, fotografier eller ljud omfattas av den rättsliga tolkningen av begreppet.[26]

Den andra beståndsdelen i definitionen är avgörande för att identifiera vilka relationer och kopplingar som är relevanta. I många situationer kan förhållandet vara tydligt, men i andra fall kanske det inte är lika uppenbart. I enlighet med detta är det viktigt att betona att för att informationen ska anses 'avse' en individ, inkluderar detta även innehållet, syftet och resultatet av behandlingen. Dessa tre beståndsdelar (innehåll, syfte, resultat) måste betraktas som alternativa förutsättningar, inte kumulativa. Beståndsdelen ”syfte” är närvarande när informationen används, eller förväntas användas, med hänsyn till alla omständigheter i det specifika fallet, för att bedöma, behandla på ett specifikt sätt eller påverka en individs ställning eller beteende. Även om beståndsdelen ”innehåll” eller ”syfte” saknas, kan information ändå anses ”avse” en enskild individ om dess användning sannolikt kommer att påverka en viss persons rättigheter och intressen, med hänsyn till alla relevanta omständigheter i det specifika fallet.[27]

När det gäller den tredje beståndsdelen ”identifierad eller identifierbar”, sker identifieringen genom vissa medel. Tolkningen fokuserar på minimikraven för att avgöra om informationen gör en individ identifierbar.[28] Det konstateras i definitionen att förordningen tillämplig oavsett om den registrerade är direkt eller indirekt identifierbar. I detta sammanhang bör det noteras att möjligheten att identifiera en individ betyder inte nödvändigtvis att kunna ta reda enbart på namnet.[29] Det är också värt att notera att kriterierna för identifieringshjälpmedel spelar en betydande roll vid bedömningen av identifieringsmöjligheter, speciellt i förhållande till syftet med databehandling.[30]

Mot bakgrund av vad definitionen tar sikte på kan en fråga uppstå om vad som händer om uppgifterna faller utanför definitionen. Detta är fallet när uppgifterna inte

[25] Artikel 16 Fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, 2012/C 326/01.

26 Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 4/2007 om begreppet personuppgifter, WP 136, s. 7.

27 Ibid, s. 9–10.

28 Se artikel 5 GDPR.

29 C-101/2001, angående tolkning av Europaparlamentetes och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om fria flödet av sådana uppgifter, p. 27.

[30] Yttrande 4/2007, s. 12–16

kan anses avse en individ, eller om individen inte kan anses identifierad eller identifierbar. En vanlig missuppfattning är att behandlingen av sådana uppgifter sker utan att ta hänsyn till dataskyddsbestämmelserna, vilket inte stämmer, dvs det inte nödvändigtvis innebär att individer saknar skydd. Även om uppgifterna faller utanför GDPR:s tillämpningsområde bör viss verksamhet ändå vara förenliga med artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna som handlar om rätten till skydd för privat- och familjeliv. Den stora betydelsen av dessa rättigheter har resulterat i en specifik reglering av icke-personuppgifter inom ramen för det fria flödet av uppgifter.[31]

Behandling av icke-personuppgifter, även kallade "andra uppgifter än personuppgifter", kan innebära liknande skyldigheter. Denna reglering är särskilt viktigt när det gäller reglering av en blandad datamängd, som består av både personuppgifter och andra typer av data, eftersom den ger en mer realistisk bild av hur behandlingen ser ut i praktiken. Detta är avgörande för den datadrivna ekonomin. Både förordningen om det fria flödet av andra data än personuppgifter och den allmänna dataskyddsförordningen syftar till att säkerställa detta och främja ett fritt flöde av information. Tillsammans lägger de grunden för en konkurrenskraftig europeisk datadriven ekonomi och möjliggör ett fritt flöde av alla typer av data inom EU. Ett exempel på blandade datamängder är datamängder i en bank, särskilt data med kundinformation och transakrionsuppgifter, såsom betaltjänster, låneavtal och tillämpningar för förvaltning av partsrelationer samt dokument med data som rör både fysiska och juridiska personer.[32] I förordningen om andra data än personuppgifter konstateras att en uppdelning av datamängden skulle resultera i en betydande minskning av dess värde. När delar bestående av icke-personuppgifter och personuppgifter är ” oupplösligt sammanlänkade” i ett blandade mängder, blir det därför nödvändigt att tillämpa dataskyddsregler och skyldigheter från GDPR på hela datamängden. Detta gäller även om andelen personuppgifter i datamängden är relativt liten. Oavsett proportionen av personuppgifter i dessa blandade mängder, kräver GDPR att dess regler fullt ut efterlevs med avseende på den delen av datamängden som innehåller personuppgifter, för att säkerställa att individens dataskyddsrättigheter upprätthålls.[33]

2.2.2 Den registrerade

Begreppet "den registrerade" definieras inte i GDPR. Utifrån definitionen av "personuppgifter" kan man härleda att "den registrerade" är den fysiska person som uppgifterna gäller, det vill säga den individ vars personuppgifter behandlas.[34]

Det är av grundläggande vikt att korrekt identifiera den registrerade för att sedan fastställa vilken individ som innehar de rättigheter som anges i förordningen, såsom rätten till information, rätten till tillgång och rätten till dataportabilitet.

[31] Se förordning Europaparlamentets och rådets förordning (EU) 2018/1805 av den 14 november 2018 om ömsesidigt erkännande av beslut om frysning och beslut om förverkande.

[32] COM (2019) final, Vägledning om förordningen om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen, s. 6–8.

[33] Ibid, s. 9–10.

[34] Se artikel 4.1 GDPR.

2.2.3 Personuppgiftsansvarig

Begreppet betraktas som både funktionellt och autonomt och kräver en tolkning som är tillräckligt bred. Det är funktionellt eftersom det syftar till att placera ansvaret där det faktiska inflytandet ligger, baserat på fakta snarare än formell analys. Det innebär att betydande vikt läggs på parternas faktiska roller. Begreppet är ett självständigt unionsrättsligt begrepp och måste tolkas utifrån syfte och sammanhang. Begreppet måste tolkas brett för att säkerställa en hög skyddsnivå och för att undvika brister och för att förhindra potentiella kringgåenden av reglerna.[35]

Begreppet personuppgiftsansvarig är av stor betydelse för tillämpningen av GDPR eftersom det fastställer vem som har ansvaret och är skyldig att följa de bestämmelser som anges i GDPR. Detta särskilt med beaktande av principerna för dataskydd[36] som riktas direkt till den personuppgiftsansvarige. Definitionen av begreppet återges i artikel 4.7 GDPR och lyder:

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

Den första byggstenen behandla typen av enhet som kan vara personuppgifts-ansvarig. Det konstateras att det inte finns någon begräsning vad gäller vilken typ av enhet som kan ha rollen som personuppgiftsansvarig. Vanligtvis är det organisationen och inte en individ inom organisationen som fungerar som personuppgiftsansvarig. Även om en särskild individ inom en organisation kan utses för att övervaka efterlevnaden av bestämmelserna, kommer den personen inte att inneha rollen som personuppgiftsansvarig utan betraktas snarare som en företrädare för den juridiska personen och agerar på dennes vägnar.[37]

Den andra byggstenen i begreppet avser det inflyttandet en personuppgiftsansvarig har över behandlingen i kraft av ett utövande a beslutanderätt. På grund av begreppets funktionella karaktär baseras bedömningen på en faktisk, snarare än en formell analys. I de flesta situationer kan det "beslutande organet" identifieras enkelt och tydligt med hänvisning till vissa rättsliga och faktiska omständigheter. Med hänsyn till detta kan identifieringen görs utifrån två kategorier. Den första kategorin hänvisar till den kontroll som härar från lagbestämmelser medan den andra tar sikte till den kontroll som härleds från faktiskt inflytande.[38]

I artikel 4.7 GDPR fastställs att "ändamål och medel" för behandlingen kan bestämmas av fler än aktör. Detta innebär att flera olika enheter kan fungera som personuppgiftsansvariga för samma behandling och samtidigt bestämmer behandlingsändamål och tillvägagångssätt. På motsvarande sätt kan en organisation

[35] Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, s. 10, och Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 1/2010 om begreppen registeransvarig och registerförare, WP 169, s. 9.

[36] Se artikel 5 GDPR.

[37] Riktlinjer 07/2020, s. 11.

[38] Ibid, s. 12-13.

fortfarande vara personuppgiftsansvarig även om den inte fattar alla beslut angående ändamål och medel.[39]

Den fjärde byggstenen hänvisar till ändamålet med den personuppgiftsansvariges inflytande. Det fastställer vad en part bör bestämma för att kvalificera sig som personuppgiftsansvarig. Ändamålet tar sikte på det förväntade resultat som är avsett eller som styr handlingar. GDPR fastställer att data måste samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det konstateras också att uppgifterna inte kan vidarebehandlas på ett sätt som är oförenligt med dessa ändamål. Den som har sådant inflytande över behandlingen av personuppgifter deltar i fastställandet av ändamålet och medlen för behandlingen i enlighet med GDPR. Fast det måste konstateras att den personuppgiftsansvarige inte kan nöja sig med att enbart fastställa ändamålet utan måste även ta beslut angående beslutsrätt.[40]

I linje med uppsatsens ämne kan ett exempel vara löneadministrationen som överför information till en bank för att genomföra lönebetalningar till anställda. Banken, i sin roll som mottagare av dessa uppgifter, avgör självständigt hur dessa uppgifter ska behandlas för att utföra sina banktjänster. Därmed anses banken vara ansvarig för behandlingen av dessa uppgifter och överföringen av information mellan löneadministrationen och banken kan ses som en utväxling av information mellan två aktörer som hanterar personuppgifter. Detta exempel, som behandlar överföringen av löneadministrationsuppgifter till en bank för lönebetalningar, återfinns också i riktlinjerna från EDPB angående begreppet personuppgiftsansvarig i GDPR.[41] Exemplet anses också förenlig med hur uttrycket ”uttryckligt medgivande” definieras i artikel 94.2 PSD2. Det bör förstås att den registrerade måste vara fullt informerad om vilka specifika kategorier av personuppgifter som kommer att behandlas. De ska också informeras om det specifika syftet för betaltjänster som deras personuppgifter kommer att användas för. Sådana upplysningar bör tydligt kunna urskiljas från övriga avtalsvillkor och det krävs att den registrerade uttryckligen samtycker till dem.[42]

Alla förutsättningar som anges för definitionen av personuppgiftsansvarig i artikel 4.7 GDPR är nära kopplade till varandra. Exempelvis har begreppet en stark koppling till ”behandling av personuppgifter”, vilket innebär att det kan appliceras på både enstaka behandlingsåtgärder och flera åtgärder. Detta kan resultera i flera aktörer som deltar i olika delar av behandlingsprocessen. Detta förtydligades i fallet Fashion ID[43], där EU-domstolen fastställde att även om en person kan vara ansvarig tillsammans med andra för behandling av personuppgifter där de gemensamt bestämmer ändamål och medel, så ansvarar de inte för tidigare eller senare åtgärder i behandlingskedjan om de inte har varit delaktiga i att fastställa ändamål eller medel för dem.[44]

[39] Ibid, s. 14.
[40] Ibid, s. 12-13.
[41] Ibid, s. 12–13.
[42] Riktlinjer 6/2020 om samspelet mellan andra betaltjänstdirektivet och dataskyddsförordningen, s. 16 – 17.
[43] Se C-40/17.
[44] Se artikel 2 d direktivet 95/74, jfr C-40/17, p. 74.

Frågan om gemensamt ansvar regleras numera i GDPR enligt artikel 26, som lyder:

> ”Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga.”

Artikeln fastställer att gemensam kontroll existerar när olika parter tillsammans bestämmer ändamål och medel för en behandling av personuppgifter. För att bedöma gemensamt personuppgiftsansvar krävs en analys av det faktiska inflytandet över behandlingen. Det bör noteras att inte all behandling där flera enheter är inblandade nödvändigtvis innebär gemensam kontroll. Det gemensamma deltagandet måste mer specifikt innefatta både fastställandet av behandlingsändamålet och behandlingssättet. Ett viktigt kriterium som måste beaktas i förhållande till ändamålen och medlen för behandlingen är huruvida behandlingen inte skulle vara möjlig utan båda parters deltanade i den meningen att varje parts behandling är oskiljbar. Fast att en av parterna inte har tillgång till de personuppgifter som behandlas är inte tillräckligt för att utesluta gemensam kontroll.[45]

I jämförelse med personuppgiftsansvariga är det viktigt att också närmare titta på definitionen av tredje part och mottagare som definieras i artikel 4.10 och 4.9 GDPR. I motsats till begreppet personuppgiftsansvarig föreskriver förordningen inte några specifika skyldigheter eller ansvar för mottagare och tredje part. En tredje part hänvisar enligt artikel 4.10 till någon som i den aktuella situationen inte är en registrerad person eller en personuppgiftsansvarig. Medan en mottagare omfattar alla som tar emot personuppgifter, oavsett om de är tredje part eller inte. Dessa begrepp kan anses relativa eftersom de beskriver olika relationer till en personuppgiftsansvarig eller ett personuppgiftsbiträde. Till exempel kan en mottagare av personuppgifter också vara personuppgiftsansvarig om de bestämmer ändamålet och medlen för behandlingen. En fråga som kan uppstå är huruvida mottagaren eller en tredje part har samma skyldigheter som den personuppgiftsansvarige.[46]

2.3 Principen om laglighet

Personuppgifter ska enligt artikel 5.1 a i GDPR behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Det betyder att artikel 5.1 GDPR och de rättsliga grunder som anges i artikel 6 GDPR är grundläggande och kumulativa. Dels måste någon av de rättsliga grunderna vara tillämpliga, dels måste samtliga principer om behandling av personuppgifter följas.

All behandling av personuppgifter måste vara laglig, korrekt och transparent i förhållande till den registrerade, vilket innebär att all datahantering behöver en rättslig grund och ska utföras på ett sätt som är öppet och begripligt för de berörda individerna. Lagligheten innebär att all behandling måste följa bestämmelserna i artikel 5–11 GDPR eftersom det slagits fast av EU-domstolen att andra bestämmelser i förordningen eller nationell rätt inte är avgörande för att uppfylla laglighetskriteriet.[47] Vad gäller korrektheten vid behandling av personuppgifter kräver förordningen en balans och rättvisa i hanteringen, där intressen som den

[45] Riktlinjer 07/2020 s. 20–21.
[46] Ibid, s. 31–32.
[47] C-60/22, p. 57–66.

registrerade och den personuppgiftsansvarige har vägts mot varandra. Begreppet "korrekt" syftar på en skälig och rimlig behandling i förhållande till de registrerade. Dessutom måste informationen och kommunikationen kring behandlingen vara lättillgänglig och lättbegriplig, och ett klart och tydligt språk måste användas. För att säkerställa korrekthet i enlighet med de rättsliga grunder som fastställs av artikel 6 GDPR måste det konstateras att vissa specifika rättigheter som tilldelas registrerade enligt GDPR gäller endast när behandlingen rättfärdigas av särskilda rättsliga grunder. Det är därför personuppgiftsansvariga bör först överväga vilka rättigheter som kan vara tillämpliga när de bedömer sina skyldigheter för dataskydd.[48]

Data ska dessutom enbart samlas in för särskilda, uttryckligen angivna och berättigade ändamål och får inte behandlas på ett sätt som är oförenligt med dessa initialt fastställda ändamål, vilket kräver en tydlig kommunikation och bestämning av syftet med insamlingen. Det är den personuppgiftsansvarige som alltid måste bestämma ändamålen med behandlingen av personuppgifterna och detta måste göras senast när personuppgifterna samlas in.[49] Det är ofta svårt att identifiera syftet med personuppgiftsbehandling för vetenskaplig forskning vid insamling. Därför bör registrerade kunna samtycka till specifika forskningsområden och projektens delar enligt etiska standarder och syftets omfattning.[50] EU-domstolen konstaterade att vidare behandling av personuppgifter för ett annat ändamål än det ursprungliga måste ha stöd i nationell rätt och vara en nödvändig och proportionell åtgärd.[51] Detta är nära kopplat till principen om uppgiftsminimering där endast adekvata och relevanta data i förhållande till de angivna ändamålen ska samlas in. Fast det kan konstateras att en personuppgiftsansvarig som mottagit personuppgifter inte är bunden av de ursprungliga ändamålen utan enbart av de ändamål de själva bestämmer vid sin insamling.[52]

Vidare ska de insamlade uppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Skäl 39 i GDPR betonar att endast nödvändig information ska samlas in för att uppnå de fastställda ändamålen. På samma sätt betonar lagringsminimeringens princip att uppgifter inte bör bevaras längre än vad som är nödvändigt för de avsedda ändamålen. Detta innebär att varje bit data ska ha en tydlig funktion och bidra till ändamålet. Principen om uppgiftsminimering kan i vissa fal kringgås där längre lagring kan vara tillåten under förutsättning att lämpliga skyddsåtgärder vidtas. Skäl 39 ger även stöd för principen om riktighet som innebär att personuppgifter måste vara korrekta och vid behov uppdaterade. För att skydda den registrerades rättigheter och integritet krävs att alla rimliga åtgärder vidtas för att snabbt rätta eller radera felaktiga uppgifter. EU-domstolen hänvisar till denna princip och har konstaterat att även felaktiga svar på ett prov kan betraktas som personuppgifter och att riktigheten av dessa uppgifter ska bedömas utifrån om de återspeglar vad som faktiskt har registrerats eller lämnats in av den registrerade, oavsett om uppgifterna i sak är korrekta eller inte.[53] Detta pekar på den bred tolkning av vad som utgör en personuppgift enligt artikel 4.1 i GDPR.

[48] Guidance on Legal Bases for Processing Personal Data, December 2019, s. 3.
[49] Se artikel 4.1 GDPR.
[50] Skäl 33 GDPR.
[51] C-268/21, p.33.
[52] Sören Öman, Dataskyddsförordningen (GDPR) m.m 2:e upplagan, 2021, s. 121.
[53] C-434/16.

Enligt denna artikel behöver en upplysning inte vara sann för att kvalificera sig som en "personuppgift". Detta förstärker principen om riktighet genom att den inkluderar en skyldighet att hantera även potentiellt felaktiga eller inaktuella uppgifter på ett korrekt och transparent sätt.[54]

Slutligen, ansvarsskyldighetsprincipen innebär att den personuppgiftsansvarige inte bara ska följa alla dessa principer utan också kunna bevisa detta genom adekvat dokumentation och procedurer. Detta skapar en ram för öppenhet och ansvarighet där organisationer måste vara proaktiva i att säkerställa och demonstrera efterlevnad av dataskyddsförordningens bestämmelser.[55]

2.4 Rätten till dataportabilitet

2.4.1 Principer och dataportabilitetens tillämpningsområden

Rätten till dataportabilitet innebär att den registrerade har rätt att få sina personuppgifter, som de har tillhandahållit den personuppgiftsansvarige, i ett strukturerat, allmänt använt och maskinläsbart format samt rätten att överföra dessa uppgifter till en annan personuppgiftsansvarig utan hinder. Denna rätt ger användarna större valmöjligheter, mer kontroll och ökat inflytande utan att påverka den registrerades övriga rättigheter.[56] Artikel 20.1 GDPR lyder:

> ”Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta [...]”

Rätten till dataportabilitet kan endast erhålls om behandlingen grundas på den registrerades samtycke enligt 6.1 a GDPR eller 9.2 a GDPR när det är fråga om särskilda kategorier. Det kan också grundas på parternas avtal enligt artikel 6.1 b GDPR. Det bör noteras att dataportabilitet inte är tillämplig på behandlingar som är nödvändiga för att utföra en uppgift av allmänt intresse eller som är en del av den personuppgiftsansvariges myndighetsutövning, och inte heller när den personuppgiftsansvarige agerar i allmänhetens intresse eller fullgör en rättslig förpliktelse. Detta innebär att ett finansinstitut inte har någon skyldighet att bevilja en begäran om dataportabilitet för personuppgifter som behandlas som ett led i dess skyldigheter att förhindra och upptäcka penningtvätt och annan ekonomisk brottslighet. Det finns god praxis som kan vara nödvändiga att beakta, även om det inte är ett rättsligt krav. Att ha processer för att hantera en begäran om dataportabilitet på ett automatiserat sätt är exempel på sådan praxis, som är i linje med de principer som reglerar rätten till dataportabilitet.[57]

Innan regler om dataportabilitet infördes genom GDPR begränsades enskilda individers möjlighet att utnyttja sin rätt till tillgång till uppgifter av det format som personuppgiftsansvariga använde när de lämnade ut den begärda informationen.

[54] Se avsnitt 2.2.1.

[55] Öman, s. 154.

[56] Artikel 29 – arbetsgruppen för skydd av personuppgifter, riktlinjer om rätten till dataportabilitet, WP 242 rev.01, s. 10.

[57] Skäl 69 GDPR, se även 29-arbetsgruppens yttrande 6/2014 om berättigade intressen, s. 47 – 48.

Artikel 20 i GDPR syftar till att ge de registrerade större inflytande över sina egna personuppgifter, utöver rätten till radering och tillgång, eftersom den underlättar för individer att flytta, kopiera eller överföra personuppgifter från en IT-miljö till en annan. Detta gäller oavsett om överföringen av data sker till de registrerades egna system eller till system som tillhör andra personuppgiftsansvariga och tredje parter. Dataportabilitet innebär även en möjlighet att förändra balansen i förhållandet mellan de registrerade och personuppgiftsansvariga, vilket i sin tur främjar syftet med dataportabilitet där enskilda ökar sin kontroll över sina personuppgifter och säkerställer att de spelar en aktiv roll i dataekosystemet. Det är viktigt att notera att en intressekonflikt kan uppstå när det gäller konkurrens mellan tjänster, även om detta inte beaktas inom ramen för GDPR.[58]

Rätten att få ut uppgifter tar sikte på en registrerad. I detta avseende kompletterar rätten till dataportabilitet rätten till tillgång till uppgifter i artikel 15 GDPR. Ett särdrag för dataportabiliteten är att den gör det lätt för de registrerade att själva hantera och vidareutnyttja personuppgifter. Uppgifter kan även överföras direkt från en annan på begäran av den registrerade när detta är tekniskt möjligt.[59] Det senare rekvisitet återfinns i artikel 20.2 GDPR, som lyder:

> ”Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.”

Rätten till dataportabilitet begränsas inte till personuppgifter som är användbara och relevanta för likdanande tjänster som tillhandhålls av konkurrenter till den personuppgiftsansvarige. Bestämmelsen garanterar rätten att få ut personuppgifter och behandla dem i enlighet med registrerades önskemål. I detta avseende är den personuppgiftsansvarige inte ansvarig för att den mottagande personuppgifts-ansvarige följer dataskyddsbestämmelserna. Den personuppgiftsansvarige måste även respektera skyldigheten att svara inom en angiven tid utan onödigt dröjsmål, och i alla fall senast en månad efter att ha mottagit begäran. Denna tidsram kan förlängas upp till tre månader vid en komplex begäran.[60] Dessa uppgifter bör naturligtvis redan vara förenliga med de principer som anges i artikel 5.1 i GDPR, vilket innebär att dataportabiliteten inte ålägger den personuppgiftsansvarige att lagra personuppgifter längre än vad som är nödvändigt.

Det krävs att en mottagande personuppgiftsansvarig måste säkerställa att de flyttbara uppgifterna som tillhandahålls är relevanta och inte överdrivet omfattande för den nya uppgiftsbehandlingen. Om information som har delats inte är relevant för den nya behandlingen bör den inte sparas och behandlas. Till exempel om en registrerad begär en överföring av uppgifter om sina banktransaktioner till en tjänst som hjälper hen att sköta sin budget, bör endast sådana uppgifter godtas och lagras som är nödvändiga och relevanta för den tjänst som tillhandahålls av den mottagande personuppgiftsansvarige.[61] Ett annat exempel är om syftet med den registrerades begäran är att ge en leverantör av kontoinformationstjänster tillgång till sin

[58] Ibid, s. 4.
[59] Ibid, s. 5.
[60] Ibid, s. 16 se även artikel 12.3 GDPR.
[61] Ibid, s. 7–8.

bankkontohistorik. I sådana fall bör denna tillgång beviljas i enlighet med bestämmelserna i PSD2.[62]

Det finns ett antal frågor som uppstår rörande vad som gäller med blandande datamängder och även blandade uppsättningar av transaktioner som innehåller personuppgifter som rör tredje part. Dessa tredje parters rättigheter behandlas närmare i artikel 20.4 GDPR, som lyder:

> ”Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt.”

Ett exempel på negativ påverkan är när överföringen av uppgifter mellan personuppgiftsansvariga begränsar tredje parters förmåga att utöva sina rättigheter enligt GDPR. Det betonas att om flera registrerade personer är inkluderade i samma uppsättning personuppgifter, bör inte rättigheten att motta dessa uppgifter påverka andra registrerades rättigheter och friheter.[63] Med hänsyn till detta villkor innebär det att när en registrerad överför sina uppgifter till en ny personuppgiftsansvarig, krävs det antingen ett nytt samtycke eller ett avtal om den nya partens databehandling.[64] Det kan argumenteras att intresseavvägning kan också vara en grund för sådan behandling. Behandling av personuppgifter utan samtycke kan vara tillåten om en intresseavvägning visar att den personuppgiftsansvariges eller en tredje parts berättigade intresse väger tyngre än den registrerades integritetsintresse.[65] Vid bedömningen av berättigade intressen kräver en noggrann och omfattande analys för att säkerställa att behandlingen av personuppgifter är proportionerlig och att de registrerades rättigheter och friheter inte överträds. Det är också viktigt att beakta vilken typ av personuppgifter som behandlas, särskilt om uppgifterna är av känslig natur.[66] Inom finansiella tjänster, särskilt betaltjänster, avser ”uppgifter från passiva parter” personuppgifter från en registrerad som inte är kund hos en specifik betaltjänstleverantör. Ett exempel är när en annan person utför betalningar till användarens konto, där uppgifter som kontonummer och transaktionsbelopp behandlas. Detta är tillåtet om det är nödvändigt för att uppfylla berättigade intressen hos den personuppgiftsansvarige eller en tredje part, förutsatt att de registrerades rättigheter och friheter respekteras. Personuppgiftsansvariga bör säkerställa att behandlingen av personuppgifter respekterar de registrerades förväntningar, vilket bidrar till ökat förtroende och säkerhet inom finanstjänstsektorn.[67] Enligt EU-domstolen krävs det, när det finns gemensamt personuppgiftsansvar, att varje involverad part uppvisar ett berättigat intresse.[68]

När det gäller att välja rättsliga grunder för behandling av personuppgifter är det nödvändigt att använda en annan rättslig grund än samtycke om överföringen innehåller data från tredje part, såsom ett berättigat intresse enligt artikel 6.1 f. Fast om behandlingen grundas på intresseavvägning enligt denna artikel, har den registrerade inte rätt till dataportabilitet.[69] Ett exempel från finanssektorn kan vara

[62] Ibid, s. 9.
[63] Se skäl 68 GDPR.
[64] Riktlinjer om rätten till dataportabilitet, WP 242 rev.01, s. 12.
[65] Artikel 6.1 f GDPR.
[66] Se avsnitt 2.5.
[67] Riktlinjer 6/2020, s. 19–12, se även skäl 87 PSD2.
[68] C- 40/17, p. 96.
[69] Öman, s. 181.

ett bankkonto som inte bara innehåller information om kontoinnehavarens egna transaktioner utan även om transaktioner utförda av andra än kontoinnehavaren. Vid en begäran om dataportabilitet brukar inte dessa tredje parters rättigheter och friheter påverkas negativt, under förutsättning att informationen fortsätter användas för samma ändamål som tidigare. Den nya mottagande personuppgiftsansvarige har inte tillåtelse att använda de överförda uppgifterna från tredje part för egna syften, såsom direktmarknadsföring.[70]

Ett ytterligare villkor som anges i bestämmelsen om rätt till dataportabilitet är att bestämmelsen begränsas till "uppgifter som den registrerade har tillhandahållit" vilket i sin tur begränsar tillämpningsområdet av bestämmelsen. Det konstateras att för att dataportabilitetsrätten ska uppnå sitt fulla värde måste "tillhandahållit" även omfatta de personuppgifter som kan observeras från användarnas aktivitet.[71] Personuppgiftsansvariga har en skyldighet att informera den registrerade om att rätten till dataportabilitet finns. Detta hänvisar inte bara till vikten av en rättvis behandling utan ger en användare möjlighet att begränsa riskerna för tredje part och all annan nödvändig dubblering av personuppgifter. Den personuppgiftsansvarige autentiserar ofta de regisserade redan innan de ingått ett avtal eller innan deras samtycke till behandlingen inhämtas.[72]

2.4.2 Särskilt om samtycke

Samtycket är en av de sex rättsliga grunder för behandling av personuppgifter som räknas upp i artikel 6.1 GDPR. För att samtycke ska kunna användas som en rättslig grund måste vissa villkor uppfylls annars kommer samtycket att vara ogiltigt som grund för behandling. Vid bedömning av hur lämpligt samtycke är som rättslig grund i förhållande till vilka rättigheter som kan vara tillämpliga vid behandling av personuppgifter under olika rättsliga grunder är det viktigt att inse att samtycke inte begränsar någon av de registrerades rättigheter.[73] När den personuppgiftsansvarige ber om samtycke bör en bedömning göras av huruvida samtliga villkor för erhållande av giltigt samtycke kommer att kunna uppfyllas.[74] Dessa villkor framgår av artikel 4.11 GDPR, som anger att ett samtycke utgörs av:

> "Varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne."

Inledningsvis innebär begreppet samtycke att individer vars uppgifter hanteras får möjlighet att kontrollera och fritt välja. En grundläggande princip är att samtycket anses ogiltigt om de berörda inte kan välja fritt, känner sig tvingade att samtycka eller drabbas av negativa konsekvenser om de avstår från att samtycka. Likaså anses samtycke inte som frivilligt om de berörda inte har möjlighet att avböja eller dra tillbaka sitt samtycke utan svårigheter. Detta är kopplat till principen om en obalanserad maktrelation mellan den personuppgiftsansvarige och de registrerade.[75]

[70] Ibid, s. 13.
[71] Ibid, s. 11.
[72] Ibid, s. 15.
[73] Guidance on Legal Bases for Processing Personal Data, December 2019, s. 3.
[74] EDPB, riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, version 1.1, s. 5.
[75] Skäl 43 GDPR.

Inom ramen för denna uppsats anses fall relevanta där samtycke endast ses som giltigt om de registrerade har verklig valfrihet och det inte föreligger någon risk för bedrägeri, trakasserier, tvång eller avsevärda negativa följder som betydande extra kostnader om samtycke inte ges.[76] Bedömningen av samtyckets frivillighet görs med hänsyn till den specifika situation där samtycke är kopplat till ett avtal eller tillhandahållandet av en tjänst. Alla former av otillbörliga påtryckningar eller påverkan på de registrerade som hindrar dem från att utöva sin fria vilja innebär generellt sett att samtycket blir ogiltigt. Samtycke som ges under villkor eller binds till avtalsbestämmelser för en tjänst där personuppgifter inte är nödvändiga, betraktas också som ogiltigt. Med hänsyn till detta får de två lagliga grunderna för behandling av personuppgifter, samtycke och avtal, inte blandas ihop.

Vidare är det viktigt att notera att samtycket inte anses uppfylla kravet på frivillighet om det inkluderar flera syften samtidigt. Det innebär att den personuppgiftsansvarige ska erhålla separat samtycke för varje syfte som beaktas. Med hänsyn till detta finns en tydlig koppling mellan frivillighetsvillkoret och de andra villkor som anges i artikel 4.11 GDPR. För att upprätthålla kraven för "specifikt" och “informerat” samtycke måste den personuppgiftsansvarige tydligt specificera de ändamål som används med tillräcklig granualaritet vid samtyckesbegäran och klart särskilja samtyckesinformation från annan data för ökad transparens och förståelse.[77] Detta är också viktigt vid bedömning av de berättigade ändamålen för den avsedda behandlingen som fastställs innan ett giltigt samtycke erhålls. Informationskravet innebär att en personuppgiftsansvarig måste säkerställa att samtycke ges på grundval av information som gör att de registrerade lätt kan förstå vad de samtycker till.[78] Till sist bygger definitionen av samtycke vidare på kravet om en otvetydig viljeyttring genom en entydigt bekräftande handling. Detta innebär att den registrerade måste ha utfört en aktiv handling för att samtycka till behandlingen i fråga. Detta gör att ett tyst godkännande av allmänna villkor inte ska betraktas som en entydigt bekräftande handling som kan utgöra samtycke till behandling av personuppgifter.[79]

2.4.3 Särskilt om avtals ingående och fullgörande

Behandlingen måste vara nödvändig för fullgörandet av avtalet med varje enskild registrerad. Det finns en koppling mellan denna rättsliga grund och samtycke som en rättslig grund där en strikt tolkning av begreppet “nödvändig för att fullgöra ett avtal” måste göras för att undvika kringgåenden av regeln om behandlingen inte är nödvändig för genomförandet av ett avtal.[80] Det är viktigt att påpeka detta är på grund av att en personuppgiftsansvarig felaktigt kan anta att undertecknandet ett avtal motsvarar samtycke i den mening som avses i artikel 6.1 a. Emellertid är dessa termer fundamentalt olika. Det är avgörande att särskilja mellan att godkänna villkoren för en tjänst för att ingå ett avtal och att ge sitt samtycke enligt artikel 6.1 a, då dessa innebär olika krav och har olika juridiska konsekvenser.[81] Den rättsliga

[76] Riktlinjer 05/2020, s. 7–9.

[77] Ibid s. 10–13, se även artikel 4.11 och 7.4 GDPR.

[78] Riktlinjer 05/2020, s. 17.

[79] Ibid, s. 18–19.

[80] Ibid, s. 11.

[81] Riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordning i samband med tillhandhållandet av onlinetjänster till registrerade, s. 7.

grunden i artikel 6.1 b gäller under två förutsättningar. Antingen behövs behandlingen för att fullgöra ett redan ingånget avtal med den registrerade eller för att förbereda ett avtal på begäran av den registrerade.

Denna rättsliga grund har en särskild koppling till ändamålsbegränsnings- och uppgiftsminimeringsprinciperna.[82] Syftet med insamlingen måste vara klar och detaljerad för att säkerställa efterlevnad av dataskyddsregler. Vaga syften som "förbättra användarupplevelsen" eller "framtida forskning" är vanligtvis inte tillräckligt specifika om de inte preciseras med fler detaljer.[83] Det måste noteras att bedömningen av huruvida artikel 6.1 b är tillämplig påverkas däremot inte av avtalets laglighet eller sammansättningen av tjänstepaketet i sig.[84] Det måste också skiljas mellan behandling som är avgörande för att uppfylla ett avtal och villkor som kopplar tjänsten till viss behandling som egentligen inte är oumbärlig för att fullgöra avtalet. Uttrycket "nödvändig för fullgörandet" innebär tydligt att det krävs något mer än bara ett villkor i avtalet.[85] Liksom kraven på specificering för samtycke, bör tillämpningen av artikel 6.1 b bedömas separat för varje fristående tjänst eller del i ett avtal som innehåller flera tjänster. Detta innebär en objektiv bedömning av vad som är nödvändigt för att fullgöra varje enskild tjänst som den registrerade aktivt har begärt eller registrerat sig för.[86]

2.5 Behandling av särskilda kategorier

GDPR bygger på att vissa kategorier av personuppgifter kräver extra skydd på grund av deras karaktär. Artikel 9 i GDPR innehåller bestämmelser om behandling av känsliga personuppgifter och fastställer ett generellt förbud mot behandling av sådana uppgifter, med vissa undantag. De uppgifter som omfattas av förbudet kan innebära en betydande påverkan på individens grundläggande rättigheter och omfattas därför av särskilda regler för att säkerställa ett förstärkt skydd. Detta innefattar behandlingen av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, medlemskap i fackföreningar, samt genetiska data, biometriska data för att unikt identifiera en person, och uppgifter om hälsa, sexualliv eller sexuell läggning.[87] Det framgår av ingressen att personuppgifter som anses särskilt känsliga bör åtnjuta särskilt skydd, eftersom behandling av sådana personuppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Det måste konstateras att detta förbud även gäller när den registrerade är personuppgiftsansvarig och behandlar känsliga personuppgifter om sig själv.[88] Det måste också konstateras att de kategorier som det talas om här måste vara personuppgifter.[89]

Behandlingen av dessa kategorier är strikt reglerad, men tillämpningen av bestämmelserna kan vara komplicerad. Vissa kategorier, som ”filosofiska

[82] Artikel 5.1 b - c GDPR.

[83] Riktlinjer 2/2019, s. 7, jfr artikel 29-gruppens yttrande 03/2013 om ändamålsbegränsning, 15–16.

[84] Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, WP 217, s. 17.

[85] Ibid, s. 8.

[86] Ibid, s. 11.

[87] Se artikel 9.1 GDPR.

[88] Skäl 51 GDPR.

[89] Se avsnitt2.2.1.

övertygelser", är svåra att definiera i praktiska sammanhang. På samma sätt kan hälsorelaterade uppgifter vara komplicerade att avgränsa på grund av den breda variationen av personuppgifter som kan inkluderas. Särskilda åtgärder krävs för att skydda sådana uppgifter, särskilt i sammanhang som behandling av hälsoinformation för försäkringsändamål.[90] Det är också otydligt hur en politisk åsikt skiljer sig från andra typer av åsikter. Detta innebär att begreppet politiska åsikter bör tolkas restriktivt, så att det inte omfattar andra åsikter.[91] Tillämpningen kan också anses komplicerad eftersom personuppgifterna som behandlas indirekt kan omfatta känsliga uppgifter. I mål C-184/20 Vyriausioji tarnybinės etikos komisija har EU-domstolen konstaterat att uppgifter som indirekt kan avslöja känsliga uppgifter om en person måste behandlas med särskild försiktighet. EU-domstolen betonar att tolkningen av dessa bestämmelser inte bara bör fokusera på uppgifternas direkta innehåll utan också på deras möjliga implikationer och konsekvenser. Detta tillvägagångssätt är i linje med syftet att säkerställa högsta möjliga skydd för personuppgifter och att beakta både de direkta och indirekta riskerna. Det praktiska genomförandet av denna tolkning kräver att den personuppgiftsansvarige genomför en riskanalys för att identifiera potentiella indirekta avslöjanden av känslig information. Denna analys leder till adekvata skyddsåtgärder för att säkerställa att även indirekta känsliga uppgifter hanteras med nödvändig försiktighet där de omfattas av artikel 9 GDPR och kräver strikta villkor för behandling.[92]

Inom ramen för GDPR kan även andra bestämmelser komma att spela in när det gäller indirekta risker. Personuppgiftsansvariga har en skyldighet genomföra adekvata åtgärder för att säkerställa och demonstrera överensstämmelse med förordningen. Denna skyldighet innefattar i vissa fall utförandet av en konsekvens-bedömning.[93] En sådan bedömning bör ses i ljuset av de övergripande skyldigheterna att hantera risker som kan påverka fysiska personers rättigheter och friheter. Det är avgörande att understryka att ansvariga för personuppgifter regelbundet måste utföra identifiering, analys, uppskattning, utvärdering, motivering och översyn av risker för att uppfylla sitt ansvar effektivt och inte enbart förlita sig på försäkringsåtgärder för att adressera dessa risker. En "risk" i detta sammanhang definieras som ett scenario som beskriver en potentiell händelse och dess förmodade konsekvenser med avseende på graden av allvar och sannolikhet.

Det måste konstateras att enligt GDPR är det inte ett krav att utföra en konsekvensbedömning för varje typ av personuppgiftsbehandling. I stället krävs sådana bedömningar endast när specifika behandlingstyper sannolikt medför en hög risk för individens rättigheter och friheter. Det är väsentligt att personuppgifts-ansvariga använder konsekvensbedömningar som ett verktyg för att systematiskt adressera och hantera potentiella risker och därigenom undvika missförhållanden vid behandlingen av känsliga data. Denna bedömning kan inkludera såväl känsliga personuppgifter som uppgifter av mycket personlig karaktär, vilka inte nödvändigtvis omfattas av kategorierna i artikel 9.[94] Vid bedömningen av

[90] Advice paper in special categories of data ("sensitive data"), s. 10.
[91] Sören Öman, Dataskyddsförordning (GDPR) m.m., s. 247.
[92] C-184/20, p. 118 - 128.
[93] Se artikel 35 GDPR.
[94] Skäl 91 GDPR.

personuppgiftsbehandlingens omfattning är det väsentligt att noggrant överväga flera faktorer. Först och främst är det antalet berörda registrerade, vilket kan specificeras antingen som ett exakt antal eller som en proportion av den aktuella populationen. Detta bidrar till en förståelse av den direkta påverkan av behandlingen. Andra faktorer som är viktiga är mängden uppgifter, variationen av de hanterade personuppgifterna och den geografiska omfattningen av behandlingen. Detta utgör en väsentlig aspekt av att bedöma de potentiella riskerna och konsekvenserna för de registrerade och påverkar således huruvida olika bestämmelser blir tillämpliga.[95]

Bland kriterierna för sådana bedömningar finns utvärdering eller poängsättning. Dessa aspekter rör vanligtvis den berörda personens arbetsprestation, ekonomiska förhållanden samt personliga preferenser och intressen. Exempelvis kan finansiella institutioner som utvärderar sina kunder mot en kreditupplysningsdatabas eller en databas för att motverka penningtvätt vara relevanta. Ett annat exempel är behandlingen av finansiella data i den mån de kan leda till betalningsbedrägerier. En oacceptabelt hög kvarstående risk är situationer där de registrerade kan drabbas av betydande eller till och med oåterkalleliga konsekvenser som de inte kan övervinna. Ett sådant scenario kan innefatta ekonomiska risker förorsakade av otillräcklig kontroll över tillgång till känslig information genom delnings- eller distributions-metoder.[96]

Det finns dock undantag från förbudet för behandling av känsliga uppgifter. Dessa undantag, som anges i artikel 9.2, gör det möjligt att behandla sådana uppgifter under specifika förutsättningar eftersom de utgör rättsliga grunder för att få behandla känsliga uppgifter. Fast för att behandlingen av sådana personuppgifter ska genomföras måste den också ha en rättslig grund enligt artikel 6 i GDPR och vara förenlig de grundläggande principerna i artikel 5.1 i GDPR. Det kan förekomma situationer där den personuppgiftsansvarige inte i förväg kan veta vilka typer av personuppgifter som kommer att behandlas. Det finns inte någon generell bestämmelse som tillåter behandlingen av känsliga uppgifter i sådana fall vilket gör att det kan vara svårt att välja vilken rättslig grund som är mest rimlig. Det är viktigt att beakta detta eftersom samtycke är ett av de undantag som tillåter behandling av känsliga uppgifter (artikel 9.1 a GDPR). Vidare måste samtycket finnas innan behandlingen av de känsliga personuppgifterna påbörjas eftersom det inte kan ges i efterhand med giltig verkan. Om samtycket inte kunde erhållas kan behandlingen fortfarande ske om det finns andra undantag som kan tillämpas. De andra undantagen omfattar bland annat behandling som är nödvändig för att skydda någons grundläggande intressen och behandling där den berörda personen själv har offentliggjort uppgifterna.[97]

2.6 Sammanfattning

Kapitlet behandlar de skyldigheter som åvilar personuppgiftsansvariga enligt GDPR och tar upp olika bestämmelser som är viktiga för att förstå bestämmelserna om

[95] WP 248 rev, 01, s. 7–11.
[96] Ibid, s. 10.
[97] Sören Öman, Dataskyddsförordning (GDPR) m.m., s. 250 – 252, se även artikel 9.2–3 GDPR.

rätten av dataportabilitet. Det betonas att personuppgifter omfattar all information som kan identifiera en individ, direkt eller indirekt. "Den registrerade" är den individ vars personuppgifter behandlas, och "personuppgiftsansvarig" är den enhet som bestämmer syften och medel för datahanteringen. Kapitlet diskuterar betydelsen av att personuppgiftsansvariga fastställer klara ändamål och medel för behandlingen av personuppgifter där all behandling av personuppgifter måste vara laglig, rättvis och transparent. Detta är avgörande för att säkerställa att datahanteringen följer de rättsliga grunderna inom GDPR. Det konstateras att rätten till dataportabilitet endast kan beviljas under en viss rättslig grund för behandling. De rättsliga grunder som diskuteras i kapitlet är samtycke och avtal ingående och fullgörande.

När det gäller finansiella tjänster är det viktigt att personuppgiftsansvariga identifierar vilka data som är nödvändiga för att tillhandahålla tjänsten och inte samlar in mer än vad som krävs. Särskilt fokus läggs på rätten till dataportabilitet, som ger individer rätten att begära ut sina personuppgifter i ett strukturerat och maskinläsbart format, samt att överföra dessa till en annan personuppgiftsansvarig. Denna rätt syftar till att stärka individens kontroll över sina data och främja konkurrens genom att underlätta byte av tjänsteleverantör. Kapitlet behandlar även de särskilda kategorier av personuppgifter enligt artikel 9 GDPR, som kräver extra skydd på grund av deras karaktär, och belyser de strikta regler och undantag som gäller för behandling av dessa uppgifter.

3 Tillgängliggörande av kunddata enligt den förslagna ramförordningen

3.1 Inledning

I syfte att adressera de luckor som finns i de befintliga dataskyddsbestämmelserna och med det åtagande som definierats i EU:s strategi för digital finansiering om att etablera ett europeiskt finansiellt dataområde, har kommissionen publicerat sitt förslag på en rättslig ram för tillgång till finansiella data. Detta förslag är inte det första i sitt slag, utan bygger på befintlig gällande rätt. Syftet med kapitlet är att svara på frågeställningen om vilka skyldigheter en datainnehavare har när det gäller att göra kunddata inom finansiella tjänster tillgängliga för dataanvändare.

Kapitlet är strukturerat i tre huvudavsnitt, där avsnitt 3.2 inleds med en bakgrund till den föreslagna förordningen. Avsnitt 3.3 beskriver FiDA:s tillämpningsområde genom att definiera nyckelbegrepp. Även om dessa begrepp är relaterade till dem som finns i GDPR, har de justerats för att passa specifikt inom ramen för den föreslagna förordningen. De begrepp som definieras i avsnittet inkluderar kunddata, datainnehavare och dataanvändare. Avsnitt 3.4 fokuserar på de specifika bestämmelserna i den föreslagna förordningen. Det är viktigt att notera att kapitlets analys inte bara bygger på källor som direkt relaterar till den nya förordningen utan även på tolkningar som är grundade på andra relevanta dataskyddsbestämmelser.

3.2 Bakgrund av den förslagna förordningen

Under 2020 slog kommissionen fast att en av prioriteringarna i dess strategi för digital finans var att främja datadriven finansiering. Idag har dataanvändare endast tillgång till finansiella data och denna brist på kontroll över data anses som ett stort problem för både organisationer och individer. Denna utmaning överensstämmer med erfarenheterna från betalsektorn, där kunder har haft svårt att förstå och hantera tillstånd för dataåtkomst. Kommissionen uttryckte sin avsikt att lägga fram ny lagstiftning, ett ramverk för öppen finans, där det bygger vidare på de befintliga bestämmelserna om öppen banking enligt PSD2, som reglerar tillgången till och behandlingen av kunddata som innehas av betaltjänstleverantörer.[98]

Förslaget är förenlig med GDPR, som ställer skyldigheter för hantering av personuppgifter och generar skyddet av dessa uppgifter. Det syftar till att skapa en ram som ska styra åtkomsten till, och användningen av, kunddata i finanssektorn. Vad som menas med att förslaget är förenligt med GDPR är att det följer samma lagliga bestämmelser som föreskrivs i GDPR. Artikel 6 föreskriver specifika skyldigheter för dataanvändare som mottar data på kundernas begäran. Endast de data som kunden har begärt utlämning av enligt artikel 5 får delges, och dessa data får endast användas för de ändamål och under de villkor som har överenskommits

[98] COM (2023) 360 final 2023/0205, s. 4.

mellan dataanvändaren och kunden. [99] Å andra sidan skulle FiDA lösa specifika problem som uppstått med dataportabilitets bestämmelser i GDPR genom att förbättra åtkomsten till finansdata för konsumenter och företag.

Trots rätten till dataportabilitet som regleras i GDPR, är datainnehavre inte juridiskt skyldiga att möjliggöra åtkomst. Detta beror på att dataåtkomst och delning kan gynna andra mer än datainnehavre, som kanske inte kan tillgodogöra sig alla fördelar från dataåteranvändning. Möjligheten för tredjepartstjänsteleverantörer att få tillgång till data på kundens begäran enligt artikel 20 i GDPR är svår att genomföra i praktiken, vilket tyder på hinder som undergräver användningen av artikel 20 GDPR inom finanssektorn. Rätten till dataportabilitet ger inte uttryckligen rätt att göra det kontinuerligt eller i realtid och är förbehållen teknisk genomförbarhet. Avsaknaden av tekniska gränssnitt som möjliggör direkt åtkomst för tredjepartsleverantörer försvårar denna rätt, vilket innebär att bristen på standardisering hindrar interoperabilitet och ökar kostnaderna för att använda överförda data. Det är också viktigt att notera att rätten till dataportabilitet är begränsad till personuppgifter som behandlas med samtycke eller för att uppfylla ett avtal, vilket utesluter data som behandlas på andra rättsliga grunder. Dessutom finns det ingen bestämmelse för icke-personliga data som är relevanta för företagskunder, vilket innebär att rätten till dataportabilitet inte täcker alla behov inom finanssektorn.[100]

Vidare även om tredjepartsleverantörer som agerar som dataanvändare kan få tillgång till kunddata genom avtal, kan många problem uppstå. Ett problem är den ojämna förhandlingsstyrkan, vilket betyder att det företag som agerar som dataanvändare befinner sig i en svagare position i värdekedjan och inte har tillräcklig förhandlingskraft gentemot datainnehavre. Vidare kan det uppstå problem kring vilka data som ska delas, definieringen av exakt omfattning och villkor för åtkomst, samt om data är av personlig natur kan detta innebära en överträdelse av GDPR eftersom det inte finns någon rättslig grund för sådan behandling.[101]

Ett ytterligare problem som uppstår på grund av begränsningarna i GDPR är att även om kunder kan förlita sig på gränssnitt som tillhandahålls av datainnehavre för att få åtkomst till sina data, finns det begränsningar. Tredjepartsleverantörer som agerar som dataanvändare utvecklar sina IT-lösningar för att använda dessa gränssnitt som åtkomstpunkter till kunddata. Detta var vanligt inom betalningsområdet innan PSD2 införde en lagstadgad skyldighet att ge åtkomst till betalkontodata. Lösningen är ineffektiv och väcker oro kring datasäkerheten. Dessutom har den negativa kostnadsimplikationer för datainnehavre. Det största säkerhetsproblemet är att det är svårt att skilja mellan auktoriserad och obehörig åtkomst. Gränssnitten är ofta inte standardiserade, vilket gör datadelning dyrare och hindrar interoperabilitet. Avsaknaden av standardisering av API:er medför att datainnehavre, även när de är skyldiga att göra data tillgängliga, gör minimala ansträngningar för att följa reglerna på grund av konkurrensskäl. Datainnehavre kan sakna incitament att utveckla högkvalitativa API:er. Komplexiteten i att integrera API:er ökar eftersom

[99] Ibid, s. 9.
[100] SWD (2023) 224 final, s. 17-18.
[101] Ibid, s. 18.

konsumenter har ett växande antal parallella avtalsförhållanden med flera datainnehavre och dataanvändare. Inom ramen för uppsatsen exponeras den finansiella sektorn för betydande ansvarsrisker vid fel eller osäkerhet kring ansvar, vilket kan avskräcka från att delta i datadelning.[102]

Förslaget fastställer att kunderna måste ha rätt att bestämma hur deras finansiella data används. Det innebär även att de ska kunna bestämma av vem deras data får användas. De kan antingen vilja begränsa tredjepartsåtkomst till sina data eller önska ge företag tillgång till sina data i syfte att erhålla finansiella tjänster och informationstjänster. Det innefattar skyldigheten för datainnehavare att dela kunddata med dataanvändare, främja standardisering av kunddata och gränssnitt, samt att främja implementeringen av högkvalitativa gränssnitt för delning av kunddata. Effektiv åtkomst innebär inte bara att tvinga datainnehavare att dela information, utan även att förbättra kvaliteten på de gränssnitt som används för datadelning, vilket är kritiskt för att säkerställa en smidig och säker dataöverföring mellan olika aktörer i den finansiella sektorn.[103]

3.3 Särskilda begrepp

3.3.1 Kunddata

Inom öppen finans omfattar begreppet kunddata de person- och icke-personuppgifter som finansiella institutioner vanligtvis samlar in, lagrar och bearbetar som en del av sin normala interaktion med kunderna.[104] Den nuvarande definitionen av "kunddata" är särskilt bred. Artikel 3(3) FiDA lyder:

> ”personuppgifter och andra data än personuppgifter som finansinstitut samlar in, lagrar och på annat sätt behandlar som en del i sin vanliga verksamhet med kunder, både data som tillhandahålls av kunder och data som genereras i samband med kundernas interaktion med finansinstituten.”

Kunder kan bestå av både fysiska individer och juridiska personer som kanske vill ge tillgång till sina data hos finansiella institutioner för att få specifika finansiella tjänster. Generellt kan kunddata definieras som varje digital representation av handlingar, fakta eller information.[105] Artikel 2.1 FiDA fastställer att kunddata avser information som är väsentliga för finansiell innovation och som innebär låg risk för finansiell exkludering. FiDA omfattar kunddata relaterad till hållbarhet för att underlätta tillgången till finansiella tjänster anpassade efter kundens hållbarhetspreferenser. Detta inkluderar data från saldo- och transaktionsuppgifter, hypotekslån, krediter, och värdepappersföretag, samt data från kreditprövningar av företag. Delning av pensionsdata är också täckt av förslaget, vilket ger pensionssparare en bättre översikt över sina rättigheter och inkomster.

Enligt FiDA omfattas även kreditkonton som erbjuder en kreditlina men som inte kan användas för betalningstransaktioner till tredje part, vilket innebär att förordningen gäller åtkomst till data som rör saldo, villkor och transaktioner för

[102] Ibid, s. 18–22.
[103] Ibid, s. 32.
[104] Artikel 3.3 COM (2023), FiDA.
[105] SWD (2023) 224 final, s. 3, se även artikel 2.1 data governance act.

hypotekslån, andra typer av lån och sparkonton.[106] Dessutom inkluderar regleringen även data om skadeförsäkringsprodukter, exklusive sjukförsäkringar, som omfattar information insamlad för att bedöma kunders krav och behov samt lämplighet och ändamålsenlighet. Data som samlas in under kreditprövningar av företag vid låneansökningar eller kreditupplysningar täcks också. Det inkluderas inte konsumenters sjukförsäkringar eller livförsäkringsprodukter, med undantag för de som är del av försäkringsbaserade investeringsprodukter.[107] Trots att artikel 3 FiDA ger en beskrivning av kategorier av personuppgifter, finns det ett behov av att specificera och klargöra dessa kategorier ytterligare. I enlighet med principen om dataminimering bör de kategorier av personuppgifter som ska göras tillgängliga enligt förslaget tydligt avgränsas, med hänsyn till arten av de finansiella tjänster och produkter som erbjuds av behöriga enheter samt riskerna för de individer vars personuppgifter skulle kunna komma att nås.[108]

Den Europeiska datatillsynsmannen (EDPS) noterar att förslaget att tillåta finansiella institutioner att få tillgång till mycket känsliga personuppgifter genom bestämmelser om datadelning, åtkomst och användning inte bara utgör ett intrång i deras grundläggande rättigheter till integritet och dataskydd, utan även kan medföra betydande risker för individers rättigheter och friheter.[109] Med tanke på denna breda definition av kunddata har EDPS påpekat att det potentiellt kan inkludera personuppgifter av mycket känsliga natur.[110] I detta avseende kan det argumenteras att sådana data delvis ka vara känsliga och omfattas av de särskilda kategorier som anges i artikel 9 GDPR.[111] Trots undantaget för vissa datakategorier kan kunddata ändå enligt Artikel 2.1 FiDA vara känsliga. Enligt kommissionens konsekvensbedömning kan vissa kunddata inkludera särskilda kategorier av personuppgifter, såsom hälsorelaterade personuppgifter. Till exempel kan pensionsrättigheter omfatta förmåner vid dödsfall, funktionshinder eller uppsägning, samt stöd vid sjukdom eller fattigdom. Hypotekslån kan också innehålla känsliga personuppgifter och kombinationen av dessa med andra finansiella tjänster kan leda till orättvis diskriminering.[112]

3.3.2 Datainnehavare

Datainnehavare är en juridisk eller fysisk person som enligt unionsrätt eller nationell lag har rätt eller skyldighet att ge åtkomst till eller dela specifika personuppgifter eller icke-personuppgifter som de kontrollerar. Inom finanssektorn betraktas de som relevanta aktörer och kan vara finansiella institutioner eller fintechföretag.[113] Definitionen utvidgas till att inkludera en rad olika typer av finansiella aktörer när de agerar som datainnehavare.[114] FiDA fastställer en specifik lista på de enheter som agerar som datainnehavare eller dataanvändare, inklusive kreditinstitut,

[106] Skäl 12–13 COM (2023), FiDA.
[107] Artikel 2 COM (2023), FiDA.
[108] SWD (2023) 224 final, s. 108.
[109] Skäl 18 COM (2023), FiDA.
[110] WP 248 rev.01, s. 10.
[111] Se 2.3.4.
[112] EDPS, opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, s. 9.
[113] SWD (2023) 224 final s. 3.
[114] Artikel 3.2 COM (2023), FiDA.

betalningsinstitut, institut för elektroniska pengar, värdepappersföretag, leverantörer av kryptotillgångstjänster, utgivare av tillgångsanknutna token, förvaltare av alternativa investeringsfonder, förvaltningsbolag för företag för kollektiva investeringar i överlåtbara värdepapper, försäkrings- och återförsäkringsföretag, försäkringsförmedlare, tjänstepensionsinstitut, kreditvärderingsinstitut, leverantörer av gräsrotsfinansieringstjänster, PEPP-sparinstitut och leverantörer av finansinformationstjänster.[115]

Det måste noteras att dataanvändare som omfattas av förordningen själva kan vara datainnehavare. De kan också vara konkurrenter till datainnehavarna eller leverantörer av tjänster inom samma sektor längre ned i kedjan.[116] Den omfattar företag som samlar in, lagrar och behandlar kunddata, exempelvis kreditinstitut, försäkringsgivare och andra finansinstitut som innehar kunddata.[117] Definitionen utvidgas till att inkludera en rad olika typer av finansiella aktörer när de uppträder i kapacitet av datainnehavare.[118]

För att säkerställa proportionalitet undantas vissa finansinstitut, såsom små tjänstepensionsinstitut med färre än 15 personer och försäkringsförmedlare som är mikroföretag eller små och medelstora företag, från denna förordning, och små och medelstora företag som är datainnehavare får tillsammans skapa ett programmeringsgränssnitt för att minska kostnaderna.[119]

3.3.3 Dataanvändare

Dataanvändare anses också vara en av de relevanta aktörerna inom finanssektorn och inkluderar finansinstitut. Detta omfattar företag som är intresserade av att få tillgång till kunddata för att erbjuda innovativa tjänster, såsom fintechbolag och andra företag som använder teknik för att tillhandahålla eller möjliggöra finansiella tjänster. Den specifika lista som FiDA fastställer i artikel 2.2 för vem som kan anses som ett finansiellt institut är densamma för både dataanvändare och datainnehavare.[120] Begreppet inkluderar även finansinstitut som erbjuder finansiella tjänster och utvecklar finansiella produkter baserade på datadelning. Dessa kan betraktas som tredjepartsleverantörer som får tillgång till kunddata som innehas av datainnehavare, baserat på kundens begäran, i syfte att tillhandahålla finansiella produkter eller tjänster för finansiell information.[121] FiDA klargör att endast de som har fått auktorisation från behöriga myndigheter kan få åtkomst till kunddata och därmed anses vara dataanvändare i den omfattning som föreslås i förordningen. En leverantör av finansiella informationstjänster måste lämna in en ansökan om auktorisation till den behöriga myndigheten i den medlemsstat där den har sitt säte. För att kunna få åtkomst till kunddata enligt artikel 5.1, måste leverantörer av finansiella informationstjänster vara auktoriserade av den behöriga myndigheten i en medlemsstat. Dessutom krävs att dessa leverantörer innehar en ansvarsförsäkring

[115] Artikel 2.2 COM (2023), FiDA.
[116] SWD (2023) 224 final, s. 13.
[117] COM (2023), FiDA, s. 1.
[118] Artikel 3.2 COM (2023), FiDA.
[119] Skäl 23 COM (2023), FiDA.
[120] Se avsnitt 3.3.2.
[121] COM (2023), FiDA, s. 1, se även SWD (2023) 224 final, s. 13.

som täcker de territorier där de har åtkomst till data, eller någon annan jämförbar garanti. De måste säkerställa att de kan täcka sitt skadeståndsansvar till följd av obehörig eller bedräglig åtkomst till eller användning av data, och att de kan täcka värdet av varje självrisk, tröskel eller avdrag från försäkringen eller den jämförbara garantin. Det är också nödvändigt att de kontinuerligt övervakar försäkringens eller garantins täckning för att säkerställa att de uppfyller dessa krav.[122]

3.4 Rättslig ram för delning av finansiella data

Syftet med FiDA är att reglera åtkomst, delning och användning av olika kategorier av kunddata inom finanssektorn.[123] Tillämpningsområdet för denna förordning täcker ett brett spektrum av kunddata inom finanssektorn. För att uppnå syftet med förordningen finns det vissa skyldigheter som åläggs på datainnehavare och dataanvändare. Dessa skyldigheter fastställer höga krav för att säkerställa att kunddata hanteras ansvarsfullt och transparent, vilket ger kunderna kontroll över sina data samtidigt som deras integritet och säkerhet skyddas. En grundläggande princip är att behandlingen av kunddata endast ska ske i den utsträckning som är strikt nödvändig med tanke på de ändamål för vilka aktuella data används.[124]

Dessa skyldigheter fastställer höga krav för att säkerställa att kunddata hanteras ansvarsfullt och transparent, vilket syftar till att ge kunder full insyn och kontroll över deras egna data samtidigt som deras integritet och säkerhet skyddas.[125]

Enligt förslaget får behöriga enheter som agerar som dataanvändare endast laglig åtkomst till kunddata som innehas av andra behöriga enheter som datainnehavare efter kundens "tillstånd". När kunden specifikt begär att deras data ska göras tillgängliga för en dataanvändare måste dataanvändaren ha en giltig rättslig grund för detta enligt GDPR.[126] EDPS påpekar att begreppet "tillstånd" definieras inte i artikel 3 i förslaget, vilket kan leda till osäkerhet kring den rättsliga grund som måste läggas till grund för behandling. Begreppet kan tolkas som antingen samtycke enligt GDPR eller som ett avtal fullgörande rättslig grund. FiDA fastställer att datainnehavare ska säkerställa att data tillhandahålls i ett standardiserat format, att kommunikationen sker säkert och att dataanvändaren visar att de har fått kundens tillstånd. Detta ska ske utan onödigt dröjsmål, kostnadsfritt, fortlöpande och i realtid för de ändamål som kunden har godkänt.[127] Det måste konstateras att dataanvändare har skyldighet att inte göra sådan delning med andra enheter inom den koncern som de kan vara en del av.[128] För att tillståndet ske på ett sätt som är förenligt med artikel 6 GDPR rekommenderar EDPS att dataanvändare tydligt specificerar vilken typ av kunddata de vill ha tillgång till i sina åtkomstförfrågningar till kunder. Detta skulle göra det möjligt för kunderna att selektivt tillåta åtkomst till vissa typer av data.[129]

[122] Artikel 12 COM (2023), FiDA.
[123] Artikel 1 COM (2023), FiDA.
[124] Artikel 7 COM (2023), FiDA.
[125] Artikel 4 COM (2023), FiDA.
[126] Skäl 10 GDPR
[127] Artikel 6.3 och artikel 5 COM (2023), FiDA.
[128] Artikel 6.4 COM (2023), FiDA.
[129] Opinion 38/2023, s. 11.

Denna skyldighet omfattar även tillhandahållande av en manöverpanel för tillstånd som gör det möjligt för kunder att övervaka och hantera sina tillstånd.[130] Det betyder att datainnehavare bör erbjuda en manöverpanel för att kunden ska kunna övervaka och hantera sina tillstånd och respektera affärshemligheter och immateriella rättigheter.[131] Manöverpanelen för tillstånd bör visa alla aktiva och tidigare tillstånd, vilket innebär att kunderna får en tydlig översikt över sina data och kan hantera sina tillstånd effektivt.[132] Panelen ska även innehålla ett register över tillstånd som har återkallats eller upphört att gälla under en period av två år. Det är datainnehavarens ansvar att se till att manöverpanelen är lättillgänglig i användargränssnittet och att informationen som presenteras är tydlig, korrekt och lättbegriplig. Det är också datainnehavarens skyldighet att informera dataanvändaren om eventuella ändringar som kunden gör i manöverpanelen, vare sig det handlar om återkallelse av ett tillstånd eller beviljande av ett nytt tillstånd avseende kunddata. Denna funktion understryker förordningens fokus på att skydda konsumenternas rättigheter och säkerställa transparens om hur kunddata hanteras och används.[133] För att säkerställa fullgörande av denna funktion rekommenderar EDPS att en bestämmelse som förbjuder att en datainnehavare inte installerar och använder tillståndspanelen enligt artikel 8 i förslaget.[134]

Skyldigheterna läggs inte endast på datainnehavaren. FiDA syftar ytterliga på att auktorisera leverantörer av finansinformationstjänster och föreskriver hur dessa leverantörer ska bedriva sin verksamhet.[135] Artikel 6 reglerar dataanvändarens skyldigheter och tar hänsyn till det andra syfte som anges i FiDA det vill säga det klargörs att endast de som har fått auktorisation från behöriga myndigheter kan få åtkomst till kunddata. Dataanvändaren får endast använda kunddata för de ändamål som kunden har godkänt och måste radera data när de inte längre behövs för dessa ändamål. EDPS rekommenderar att förordningen införa ett krav för dataanvändare att i sina åtkomstförfrågningar tydligt ange vilka specifika typer av kunddata de vill få tillgång till. Detta skulle göra det möjligt för kunder att selektivt ge åtkomst till vissa typer av data. Kravet, tillsammans med GDPR:s transparenskrav. Detta är särskilt viktigt vid bedömning av hur känsliga de specifika datamängderna är.[136]Vidare ställs krav på att dataanvändare inte får använda kunddata för icke godkända ändamål, måste vidta lämpliga säkerhetsåtgärder och inte sprida kunddata inom en företagsgrupp utöver vad som är nödvändigt. För att erhålla auktorisation för leverantörer av finansiella informationstjänster måste en leverantör framställa en ansökan till den behöriga myndigheten i den medlemsstat där företaget är baserat. Ansökan innehåller flera viktiga dokument och information för bedömning.[137] Om åtkomst till data ges mot ersättning bör kostnaderna fördelas rättvist mellan datainnehavare och dataanvändare i datavärdekedjan. För att säkerställa proportionalitet för mindre marknadsaktörer, såsom små och medelstora företag, bör

[130] Artikel 5 COM (2023), FiDA.
[131] Artikel 6.3 och artikel 5 COM (2023), FiDA.
[132] Skäl 22 COM (2023), FiDA.
[133] Artikel 8 COM (2023), FiDA.
[134] Opinion 38/2023, s. 11, skäl 54 COM (2023), FiDA.
[135] Artikel 1 COM (2023), FiDA.
[136] Opinion 38/2023, s. 12.
[137] Artikel 12 COM (2023), FiDA.

ersättningen begränsas till att endast täcka de faktiska kostnaderna för att ge åtkomst till data.[138]

3.5 Sammanfattning

Kapitlet undersöker kommissionens förslag om en rättslig ram för tillgång till finansiella data, FiDA, som syftar till att etablera ett säkert ramverk för datadelning och stärka konsumenters kontroll över sina data. FiDA är utformat för att ge dataanvändare effektiv åtkomst till kunddata, vilket för närvarande är begränsat utanför betalningsområdet. Denna föreslagna förordning innebär en skyldighet för datainnehavare att dela kunddata och främja implementeringen av tekniska metoder för delning.

FiDA understryker att skyldigheterna inte enbart gäller datainnehavare utan även auktoriserade leverantörer av finansiella informationstjänster, som måste följa strikta regler för hantering av kunddata. Begreppet kunddata är brett definierat för att inkludera en mängd finansiell information om bland annat investeringar, kreditkonton och andra banktjänster som inte täcks av PSD2. Denna breda definition kan inkludera känsliga personuppgifter, vilket väcker frågor om hur dessa data bör klassificeras och hanteras i enlighet med dataskyddsregler.

De berörda aktörerna inkluderar traditionella banker, försäkringsbolag samt tredjepartsleverantörer av finansiella tjänster. Datainnehavare är skyldiga att dela data säkert och i enlighet med GDPR. FiDA kräver att dataanvändare har tillstånd från relevanta myndigheter och följer strikta regler kring hantering och användning av kunddata.

Genom att främja datadelning och stärka konsumenters kontroll över sina data kan FiDA bidra till finansiell innovation och ökad konkurrens inom sektorn. Förslaget betonar behovet av teknisk och regulatorisk interoperabilitet för dataåtkomst och infrastruktur, vilket är avgörande för att uppnå de övergripande målen med öppen finans och skapa en dynamisk och konkurrenskraftig dataekonomi inom EU.

[138] Skäl 29 COM (2023), FiDA.

4 Slutsats och analys

Med den snabbt växande mängden data i världen och den digitala teknikens genomgripande påverkan på ekonomin och samhället, är det av yttersta vikt att förstå de skyldigheter som åvilar de som behandlar olika typer av uppgifter, särskilt personuppgifter. GDPR, sedan dess införande, har spelat en avgörande roll för hur personuppgifter skyddas och hanteras inom EU. För finansiella tjänster innebär detta specifika skyldigheter för personuppgiftsansvariga när det gäller hantering av kunddata. Dessa skyldigheter inkluderar bland annat laglig behandling, integritetsskydd, transparens och säkerhet i hanteringen av personuppgifter. Det är viktigt att dessa skyldigheter följs på ett sätt som inte minskar de rättigheter som den registrerade har enligt GDPR.

Inom ramen för GDPR har personuppgiftsansvariga betydande skyldigheter när det gäller att göra kunddata inom finansiella tjänster tillgänglig för dataanvändare. GDPR fastställer att personuppgiftsansvariga har en skyldighet att lagligt behandla personuppgifter. Principen om laglighet kräver att all personuppgiftsbehandling ska ha en rättslig grund, vilket innebär att den personuppgiftsansvariga måste kunna hänvisa till en specifik rättslig grund för varje behandling av personuppgifter, inklusive vid överföring av data till en annan tjänst eller aktör. De rättsliga grunderna som ofta är relevanta inom finansiella tjänster inkluderar samtycke från den registrerade och att behandlingen är nödvändig för att fullgöra ett avtal där den registrerade är part. Personuppgiftsansvariga är enbart skyldiga att tillhandahålla den data som antingen har tillhandahållits av den registrerade själv eller som har genererats av dennes aktiviteter inom de finansiella tjänsterna. Detta inkluderar inte data som personuppgiftsansvariga har skapat eller härlett från den ursprungliga informationen, såsom analyser eller kreditbedömningar. Denna distinktion är kritisk för att förstå omfattningen av dataportabilitetens tillämpningsområde. Personuppgiftsansvariga har en skyldighet att se till att överföringen sker på ett säkert sätt och att de tekniska formaten är interoperabla, men de är inte ansvariga för att den mottagande personuppgiftsansvarige följer dataskyddsbestämmelserna vid rätten till dataportabilitet. Vidare är det värt att notera att personuppgiftsansvariga måste informera individer om deras rättigheter när det gäller dataportabilitet. Dessa skyldigheter är emellertid endast tillämpliga om det är tekniskt möjligt.

En fråga som kan uppstå är vem som är den personuppgiftsansvarige och som måste uppfylla skyldigheterna? Är det den som lämnar ut uppgifterna eller den som mottager dem? Dessutom kan det finnas situationer där gemensamt personuppgiftsansvar föreligger. Dessa frågor blir särskilt viktiga vid bestämmande av ändamålet för behandlingen. Bestämmelsen stadgar att den personuppgiftsansvarige har en skyldighet att överföra personuppgifter till en annan personuppgiftsansvarig. I förhållande till principen om laglighet är det den personuppgiftsansvarige som bestämmer ändamålen för behandlingen av

personuppgifter. Vidare finns det ingen begränsning vad gäller vilken typ av enhet som kan anses vara en personuppgiftsansvarig.

När data överförs från en personuppgiftsansvarig till en annan, måste den nya mottagaren säkerställa att behandlingen av de mottagna uppgifterna är relevant och proportionell för det ändamål för vilket de mottages. Detta kan tolkas på två sätt: antingen att den ursprungliga personuppgiftsansvarige måste bestämma ändamålet eftersom denne anses som den ursprungliga personuppgiftsansvarige, eller att den mottagande personuppgiftsansvarige har möjlighet att bestämma ändamålet för de personuppgifter som hen har mottagit. Anledningen till att den mottagande personuppgiftsansvarige kan bestämma ändamålet är att överföringen av personuppgifter till en ny mottagare anses som en ny behandling av uppgifterna. Enligt GDPR måste varje ny behandling av personuppgifter ha ett specifikt och lagligt ändamål för att anses laglig. Det krävs att en mottagande personuppgiftsansvarig säkerställer att de uppgifter som tillhandahålls är relevanta och inte överdrivet omfattande för den nya uppgiftsbehandlingen. Detta kan tolkas som att det är mottagaren som måste bestämma det nya ändamålet. Om de mottagna uppgifterna inte är relevanta för den nya behandlingen bör de inte sparas och behandlas. Den mottagande personuppgiftsansvarige måste dock säkerställa att det nya ändamålet är förenligt med de allmänna principerna för dataskydd och att nödvändiga åtgärder vidtas för att skydda de registrerades rättigheter och friheter.

Det är viktigt att notera att ifall den mottagande personuppgiftsansvarige bestämmer ett nytt ändamål för behandlingen, måste de registrerade informeras om det nya ändamål och hur deras personuppgifter kommer att användas. Detta säkerställer transparens och att de registrerade kan utöva sina rättigheter enligt GDPR. Däremot har den mottagande personuppgiftsansvarige inte tillåtelse att använda de överförda uppgifterna från tredje part för egna syften, såsom direktmarknadsföring. Med hänsyn till detta villkor innebär det att när en registrerad överför sina uppgifter till en ny personuppgiftsansvarig, krävs det antingen ett nytt samtycke eller ett avtal om den nya partens databehandling. Det betyder att medan den ursprungliga personuppgiftsansvarige har ansvar för att fastställa ändamålet för den initiala insamlingen och behandlingen av personuppgifterna, måste den mottagande personuppgiftsansvarige ta ansvar för att säkerställa att den nya behandlingen uppfyller kraven på laglighet enligt GDPR.

En sådan bedömning av de olika personuppgiftsansvarigas skyldigheter kan vara av mindre betydelse i förhållande till den föreslagna förordningen. Detta beror på att FiDA fastställer särskilda skyldigheter för varje part som är involverad i processen med överföring och åtkomst till personuppgifter, nämligen datainnehavaren och dataanvändaren. Det finns flera andra utmaningar med att implementera rätten till dataportabilitet i praktiken inom ramen för GDPR, såsom avsaknad av tekniska gränssnitt och standardisering, vilket hindrar interoperabilitet och ökar kostnaderna för datadelning. Dessutom fokuserar rätten till dataportabilitet endast på personuppgifter, vilket inte är tillräckligt med tanke på den komplexa naturen av finansiella uppgifter som innehåller olika kategorier av data, inklusive så kallad kunddata.

Enligt FiDA åläggs datainnehavare specifika skyldigheter för att säkerställa ansvarsfull hantering av kunddata inom finanssektorn. Först och främst måste datainnehavare tillhandahålla kunddata till dataanvändare på begäran. Detta kräver att datainnehavare upprättar robusta system och processer för att extrahera, överföra och dela data på ett effektivt och säkert sätt. Dessa system måste vara anpassade för att garantera att data inte förloras eller manipuleras under överföringsprocessen. För att skydda kunddata mot obehörig åtkomst, förlust eller skada måste datainnehavare säkerställa att alla överföringar sker med användning av kryptering och säkra överföringsprotokoll. En annan viktig skyldighet är att tillhandahålla data i ett standardiserat format för att säkerställa kompatibilitet och enkel integration för dataanvändare. Enligt FiDA är det också nödvändigt för datainnehavare att erbjuda en manöverpanel för tillstånd som gör det möjligt för kunder att övervaka och hantera sina tillstånd. Datainnehavare måste se till att manöverpanelen är lättillgänglig och att informationen presenteras på ett tydligt och lättbegripligt sätt. Det är också deras ansvar att informera dataanvändaren om eventuella ändringar som kunden gör i manöverpanelen.

En fråga som kan uppstå i detta sammanhang och med tanke på samspelet mellan FiDA och GDPR är vad som menas med "tillstånd". I ett yttrande från EDPS påpekas en oklarhet i förslaget vad gäller skillnaden mellan "tillstånd" och de rättsliga grunderna för behandling enligt GDPR, nämligen "samtycke", "uttryckligt samtycke" eller "nödvändighet för att fullgöra ett avtal". Skäl 48 fastställer att en kund ger sitt tillstånd innebär inte att dataanvändare inte måste fullgöra de skyldigheter som beskrivs i artikel 6 GDPR. EDPS rekommenderar att den klargöras. Begreppet är inte nytt men saknar definition i förslaget. Enligt en annan dataskyddsbestämmelse används "tillstånd" för icke-personuppgifter, vilket innebär att en registrerad person skulle ge samtycke vid en dataomvandling, medan en juridisk person kan ge tillstånd för behandling av sina icke-personuppgifter.[139] Detta anses rimligt eftersom GDPR:s rättsliga grunder endast omfattar fysiska personer och deras personuppgifter, medan FiDA även inkluderar icke-personuppgifter. Vid överföring av kunddata från en juridisk person, som ofta involverar personuppgifter från fysiska personer, kan ett tillstånd från den juridiska personen inte ge datainnehavare rätt att överföra kunddata till en annan användare. Detta leder till en komplex situation där skillnaden mellan tillstånd och rättsliga grunder för behandling måste tydliggöras för att undvika att GDPR:s bestämmelser kringgås.

Vidare finns det flera frågor som kan uppstå när man analyserar samspelet mellan GDPR och FiDA. En viktig definition att diskutera i detta sammanhang är "kunddata" och hur väl det motsvarar begreppet personuppgifter enligt GDPR. FiDA definierar "kunddata" som avgörande för finansiell innovation och inkluderar ett brett spektrum av finansiell information relaterad till investeringar, kreditkonton och andra banktjänster. Detta omfattar både personuppgifter och icke-personuppgifter, vilket kräver en nyanserad förståelse av hur dessa olika datakategorier ska hanteras i förhållande till GDPR. Personuppgifter, enligt GDPR, innefattar all typ av information som direkt eller indirekt kan kopplas till en levande person. Banksektorn exemplifierar detta genom bedömningar av låntagarens pålitlighet, vilket även är relevant inom försäkringsbranschen som omfattas av FiDA. Om rekvisiten inte

[139] Skäl 6 och 9, 2022/868 Data Governence Act.

uppfylls, anses uppgifterna vara andra än personuppgifter, men dessa uppgifter saknar inte skydd helt och kan inte överföras fritt. De regleras av förordningen om en ram för det fria flödet av andra data än personuppgifter. Denna reglering är särskilt viktig när det gäller blandade datamängder, vilket ger en mer realistisk bild av hur behandlingen ser ut i praktiken. Ett exempel på blandade datamängder är data i banksektorn, som kan innefatta kundinformation och transaktionsuppgifter som betaltjänster och låneavtal. Förordningen om andra data än personuppgifter konstaterar att en uppdelning av datamängden skulle minska dess värde betydligt, vilket gör att GDPR:s regler måste tillämpas på hela datamängden. Detta är avgörande för att säkerställa att individens dataskyddsrättigheter upprätthålls, oavsett proportionen av personuppgifter i dessa blandade mängder.

Rätten till dataportabilitet enligt GDPR är begränsad till de personuppgifter som den registrerade har tillhandahållit den personuppgiftsansvarige. För att uppnå sitt fulla värde måste "tillhandhållandet" även omfatta de personuppgifter som observeras från användarnas aktivitet. Här uppstår frågor om blandade datamängder och transaktioner som innehåller personuppgifter rörande tredje part. Artikel 20.4 GDPR behandlar tredje parters rättigheter och friheter och fastställer att sådana rättigheter inte får påverkas negativt. FiDA specificerar att kunddata inkluderar både personliga och icke-personliga transaktionsdata som uppstår från kundernas interaktion med finansiella tjänsteleverantörer. Kunder kan bestå av både fysiska individer och juridiska personer som vill ha tillgång till sina data för specifika finansiella tjänster. Trots att artikel 3 FiDA beskriver kategorier av personuppgifter, finns det behov av ytterligare specificering och klargörande. Principen om dataminimering i FiDA kräver att dessa kategorier tydligt avgränsas med hänsyn till de finansiella tjänsternas natur. EDPS noterar att förslaget att tillåta finansiella institutioner att få tillgång till mycket känsliga personuppgifter genom datadelning väcker diskussion om hur begreppet känsliga uppgifter definieras i förhållande till GDPR. GDPR ställer strikta krav på personuppgiftsansvariga att känsliga uppgifter inte får behandlas utan undantag, såsom samtycke eller avtalsfullgörande. Det kan argumenteras att känsliga uppgifter i FiDA kan medföra indirekta risker. Dessa risker definieras som scenarion som beskriver potentiella händelser och deras förmodade konsekvenser, baserat på graden av allvar och sannolikhet. Perspektivet att överväga är om begreppet känsliga uppgifter enligt FiDA verkligen återspeglar definitionen i GDPR. GDPR fastställer skyldigheter för personuppgiftsansvariga att säkerställa att känsliga uppgifter skyddas och endast behandlas under specifika förutsättningar. De känsliga uppgifterna som hanteras inom FiDA kan betraktas som att inneha indirekta risker, vilket innebär att potentiella händelser och deras konsekvenser måste beaktas noggrant för att säkerställa att dataskyddsreglerna följs fullt ut.

Samspelet mellan GDPR och FiDA är avgörande för att förstå den framväxande strukturen av dataskydd inom finansiella tjänster. GDPR etablerade grunden för dataskydd genom att införa omfattande principer och skyldigheter för alla sektorer, såsom laglighet, rättvisa, transparens, dataminimering, begränsning av lagring, säkerhet och ansvarighet. FiDA bygger vidare på dessa grundläggande principer men introducerar specifika krav och skyldigheter anpassade till den unika miljön och riskprofilen inom finanssektorn. FiDA:s införande av rätten till dataportabilitet och

de tekniska krav som detta medför, såsom standardisering och interoperabilitet, är en central del av samspelet med GDPR.

Avslutningsvis, sedan GDPR:s införande har rätten till dataportabilitet haft begränsad användning, både inom finansiella tjänster och generellt. Denna rättighet är svår att erhålla, främst på grund av att det saknas starka incitament för finansiella institutioner att underlätta portabilitet. Erfarenheterna från PSD2 visar att FiDA kan förenkla erhållandet av dataportabilitet. FiDA bygger vidare på PSD2:s ramverk för öppen bankverksamhet och syftar till att skapa ett mer effektivt och säkert system för delning av kunddata. Dessutom finns det en betydande oklarhet bland de registrerade om denna rättighet, vilket leder till låg tillit och begränsad efterfrågan. en En av de största utmaningarna är avsaknaden av rättsfall på området, vilket bidrar till osäkerhet kring hur reglerna ska tolkas och tillämpas. Denna brist på juridisk praxis gör det svårt att dra definitiva slutsatser om effektiviteten av rätten till dataportabilitet i dagsläget. Å ena sidan begränsar detta möjligheten att förstå hur rätten till dataportabilitet kan förbättras och implementeras mer effektivt i framtiden i förhållande till FiDA. Å andra sidan kan det diskuteras huruvida avsaknaden av rättspraxis faktiskt kan ses som en fördel i vissa avseenden. Utan fastställda rättsfall finns en större flexibilitet och anpassningsbarhet för FiDA:s implementering, vilket kan möjliggöra en mer dynamisk och kontextspecifik tillämpning av reglerna. Detta kan i sin tur medföra att FiDA kan effektivt adressera och anpassa sig till de specifika behov och utmaningar som olika aktörer inom finanssektorn ställs inför, utan att vara begränsad av tidigare rättsliga praxis.

Källförteckning

Offentligt tryck

Europeiska unionen

Artikel 29 – arbetsgruppen för skydd av personuppgifter, riktlinjer om rätten till dataportabilitet, WP 242 rev.01.

Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 1/2010 om begreppen registeransvarig och registerförare, WP 169.

Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 4/2007 om begreppet personuppgifter, WP 136.

Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, WP 217.

Artikel 29 – arbetsgruppen för skydd av personuppgifter, yttrande 03/2013 om ändamålbegränsning, WP 203.

Artikel 29 – arbetsgruppen för skydd av personuppgifter, riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, WP 248 rev. 01.

Article 29 – data protection working party, Advice paper on special categories of data (“sensitive data”), Ref. Ares (2011)444105 - 20/04/2011

Commission Staff Working Document**,** Impact Assessment Report, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554**,** SWD(2023) 224 final.

Data Protection Commission, Guidance on Legal Bases for Processing Personal Data, December 2019.

Direktiv europaparlamentets och rådets direktiv (EU), 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.

EDPB, riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, version 1.1

EDPB, riktlinjer 06/2020 om samspelet mellan andra betaltjänstdirektivet och dataskyddsförordningen, version 2.0.

EDPB, riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde, version 2.0.

EDPB, riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, version 2.0.

EDPS, opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access.

Europaparlamentets och Rådets förordning (EU), DIREKTIV
EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2015/2366
av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.

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), 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen.

Europaparlamentets och Rådets förordning (EU), 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724.

Europaparlamentets och Rådets förordning (EU), 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828.

Fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, 2012/C 326/01.

Meddelande från kommissionen till europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén, en EU-strategi för data, COM (2020) 66 final.

Proposal for a regulation of the European parliament and of the council on a framework for Financial Data Access and amending Regulations (EU), COM (2023) 360 final, 2023/0205 (COD).

Litteratur

Bernitz, Ulf, Mia Carlsson, Lars Heuman, Madeleine Leijonhufvud, Cecilia Magnusson Sjöberg, Peter Seipel, and others, *Finna Rätt: Juristens Källmaterial Och Arbetsmetoder*, upplaga 16, Norstedts Juridik, 2023.

Kleineman, Jan (2018) ’Rättsdogmatisk metod’, i: Nääv, Maria, and Mauro Zamboni, *Juridisk Metodlära*, upplaga 2, Lund: Studentlitteratur, 2018, s. 21–46.

Reichel, Jane (2018) ’EU-rättslig metod’, i: i: Nääv, Maria, and Mauro Zamboni, *Juridisk Metodlära*, upplaga 2, Lund: Studentlitteratur, 2018, s. 109–142.

Öman, Sören, *Dataskyddsförordningen (GDPR) M.M.: En Kommentar*, upplaga 2, Stockholm: Norstedts Juridik, 2021.

Rättsfall

Europeiska unionens domstol, CJEU

Dom den 6 november 2003 mål C-101/2001, Lindqvist, ECLI:EU:C2002:513.

Dom den 20 december 2017 mål C-434/16, Nowak, ECLI:EU:C:2017:994.

Dom den 29 juli 2019 mål C-40/17, Fashion ID, ECLI:EU:C:2019:629.

Dom den 1 augusti 2022 mål C-184/20, Vyriausioji tarnybinės etikos komisija, ECLI:EU:C:2022:601.

Dom den 2 mars 2023 mål C-268/21, Norra Stockholm Bygg, ECLI:EU:C:2023:145.

Dom den 4 maj 2023 mål C-60/22, Bundesrepublik Deutschland, ECLI:EU:C:2023:373.