Riktlinjer 6/2020 om samspelet mellan andra betaltjänstdirektivet och dataskyddsförordningen

Version 2.0

Antagna den 15 december 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versionshistorik

Version 2.0	15 december 2020	Antagande av riktlinjerna efter samråd med allmänheten
Version 1.0	17 juli 2020	Antagande av riktlinjerna inför offentligt samråd

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i arbetsordningen, och

av följande skäl:

1) Den allmänna dataskyddsförordningen tillhandahåller ett enhetligt regelverk för behandling av personuppgifter inom hela EU.

2) Genom andra betaltjänstdirektivet (Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 23 december 2015, *andra betaltjänstdirektivet*) upphävs direktiv 2007/64/EG. Vidare fastställs nya bestämmelser för att säkerställa rättssäkerhet för konsumenter, näringsidkare och företag inom betalningskedjan samt moderniseras den rättsliga ramen för marknaden för betaltjänster[2]. Medlemsländerna skulle ha införlivat andra betaltjänstdirektivet i den nationella lagstiftningen senast den 13 januari 2018.

3) En viktig del av andra betaltjänstdirektivet utgör införandet av en rättslig ram för nya tjänster för betalningsinitiering och kontoinformationstjänster. Direktivet gör det möjligt för dessa nya betaltjänstleverantörer att erhålla tillgång till registrerades betalkonton för att kunna tillhandahålla nämnda tjänster.

4) Vad gäller dataskydd ska all behandling av personuppgifter enligt artikel 94.1 i andra betaltjänstdirektivet, inbegripet tillhandahållande av information om behandlingen enligt detta direktiv utföras i enlighet med dataskyddsförordningen[3] och förordning (EU) 2018/1725.

5) I skäl 89 i andra betaltjänstdirektivet anges att när personuppgifter behandlas med avseende på direktivet bör det exakta syftet anges, tillämplig rättslig grund åberopas, relevanta säkerhetskrav i dataskyddsförordningen följas och principerna om nödvändighet, proportionalitet, ändamålsbegränsning och proportionerlig lagringstid för uppgifter tillämpas. Dessutom bör inbyggt uppgiftsskydd och dataskydd som standard ingå i alla databehandlingssystem som utvecklas och används inom ramen för andra betaltjänstdirektivet[4].

6) I skäl 93 i andra betaltjänstdirektivet anges att leverantörerna av betalningsinitieringstjänster och leverantörerna av kontoinformationstjänster, å ena sidan, och den kontoförvaltande betaltjänstleverantören, å andra sidan, bör iaktta nödvändiga dataskydds- och säkerhetskrav som fastställs eller som avses i detta direktiv eller som ingår i tekniska standarder för tillsyn.

[1] Hänvisningar till ”medlemsstater” i detta dokument bör förstås som hänvisningar till ”medlemsstater i EES”.
[2] Skäl 6 i andra betaltjänstdirektivet.
[3] Eftersom andra betaltjänstdirektivet antogs före dataskyddsförordningen hänvisas fortfarande till direktiv 95/46. I artikel 94 i dataskyddsförordningen föreskrivs att hänvisningar till det upphävda direktiv 95/46 ska anses som hänvisningar till dataskyddsförordningen.
[4] Skäl 89 i andra betaltjänstdirektivet.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1. INLEDNING

1. Genom andra betaltjänstdirektivet har ett antal nyheter införts på området för betaltjänster. Medan detta skapar nya möjligheter för konsumenter och ökar insynen inom detta område medför tillämpningen av andra betaltjänstdirektivet att det uppkommer vissa frågor och farhågor vad gäller kravet på att registrerade ska behålla full kontroll över sina personuppgifter. Den allmänna dataskyddsförordningen (*dataskyddsförordningen)* är tillämplig på behandling av personuppgifter, inbegripet behandling som genomförs i samband med betaltjänster såsom de definieras i andra betaltjänstdirektivet[5]. Således ska personuppgiftsansvariga som är verksamma inom det område som omfattas av andra betaltjänstdirektivet alltid säkerställa att de principer om skydd av personuppgifter som föreskrivs i artikel 5 i dataskyddsförordningen samt de relevanta bestämmelserna i direktivet om integritet och elektronisk kommunikation följs[6]. Samtidigt som andra betaltjänstdirektivet[7] och de tekniska tillsynsstandarderna för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder (*de tekniska tillsynsstandarderna*[8]) innehåller vissa bestämmelser om dataskydd och datasäkerhet har det uppstått osäkerhet beträffande tolkningen av dessa bestämmelser samt samspelet mellan den allmänna ramen för dataskydd och andra betaltjänstdirektivet.

2. Den 5 juli 2018 utfärdade dataskyddsstyrelsen en skrivelse om andra betaltjänstdirektivet, i vilken styrelsen klargjorde frågor som rörde skydd av personuppgifter i förhållande till andra betaltjänstdirektivet, särskilt behandling av personuppgifter från icke-avtalsslutande parter (uppgifter från passiva parter) från leverantörer av kontoinformationstjänster och leverantörer av betalningsinitieringstjänster, förfarandena för att lämna och återkalla samtycke, de tekniska tillsynsstandarderna och samarbete mellan kontoförvaltande betaltjänstleverantörer när det gäller säkerhetsåtgärder. Det förberedande arbetet med dessa riktlinjer har omfattat insamling av synpunkter från berörda parter, både skriftligt och vid en sammankomst med berörda parter, för att identifiera de mest brådskande utmaningarna.

3. Syftet med dessa riktlinjer är att tillhandahålla ytterligare vägledning om dataskyddsaspekter i samband med andra betaltjänstdirektivet, i synnerhet om förhållandet mellan de relevanta bestämmelserna i dataskyddsförordningen och i andra betaltjänstdirektivet. Tyngdpunkten i dessa riktlinjer ligger på behandlingen av personuppgifter från leverantörer av kontoinformationstjänster och betalningsinitieringstjänster. I detta dokument behandlas villkor för att bevilja tillgång till betalkontoinformation från kontoförvaltande betaltjänstleverantörer och för behandling av personuppgifter från leverantörer av betalningsinitieringstjänster och

[5] Artikel 1.1 i dataskyddsförordningen.
[6] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37.
[7] Artikel 94 i direktivet osv.
[8] Kommissionens delegerade förordning (EU) 2018/389 av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder (Text av betydelse för EES.), C/2017/7782, EUT L 69, 13.3.2018, s. 23, finns på https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32018R0974&from=SV

kontoinformationstjänster, inbegripet villkor och skyddsåtgärder när det gäller behandling av personuppgifter från leverantörer av betalningsinitieringstjänster och kontoinformationstjänster för andra ändamål än de för vilka de ursprungligen samlades in, särskilt när uppgifterna har samlats in inom ramen för tillhandahållandet av en kontoinformationstjänst[9]. I dokumentet behandlas även olika begrepp i samband med uttryckligt samtycke enligt andra betaltjänstdirektivet och dataskyddsförordningen, behandling av uppgifter från passiva parter, behandling av särskilda kategorier av personuppgifter från leverantörer av tjänster för betalningsinitiering och kontoinformationstjänster, tillämpning av de centrala principerna för dataskydd som fastställs i dataskyddsförordningen, inbegripet uppgiftsminimering, öppenhet, ansvar och säkerhetsåtgärder. Andra betalskyddsdirektivet omfattar tvärfunktionellt ansvar inom bland annat områdena för konsumentskydd och konkurrensrätt. Dessa riktlinjer omfattar inte överväganden som rör dessa rättsområden.

4. För att underlätta läsningen av dessa riktlinjer tillhandahålls de centrala definitioner som används i detta dokument nedan.

1.1 Definitioner

Leverantör av kontoinformationstjänst: leverantören av en onlinetjänst för att tillhandahålla sammanställd information om ett eller flera betalkonton som betaltjänstanvändaren innehar hos antingen en annan betaltjänstleverantör eller hos fler än en betaltjänstleverantör.

Kontoförvaltande betaltjänstleverantör: en betaltjänstleverantör som tillhandahåller och förvaltar ett betalkonto för en betalare.

Uppgiftsminimering: en dataskyddsprincip enligt vilken personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Betalare: en fysisk eller juridisk person som är betalkontoinnehavare och som godkänner en betalningsorder från detta betalkonto eller, i avsaknad av detta, en fysisk eller juridisk person som lämnar en betalningsorder.

Betalningsmottagare: en fysisk eller juridisk person som är den avsedda mottagaren av medel som har omfattats av en betalningstransaktion.

Betalkonto: ett konto i en eller flera betaltjänstanvändares namn för användning vid genomförandet av betalningstransaktioner.

Leverantör av betalningsinitieringstjänster: leverantören av en tjänst för att initiera en betalningsorder på begäran av betaltjänstanvändaren med avseende på ett betalkonto hos en annan betaltjänstleverantör.

Betaltjänstleverantör: ett organ som avses i artikel 1.1 i andra betaltjänstdirektivet[10] eller en fysisk eller juridisk person som omfattas av ett undantag enligt artiklarna 32 eller 33 i nämnda direktiv.

[9] En kontoinformationstjänst är en onlinetjänst för att tillhandahålla sammanställd information om ett eller flera betalkonton som betaltjänstanvändaren innehar hos antingen en annan betaltjänstleverantör eller hos fler än en betaltjänstleverantör.

[10] I artikel 1.1 i andra betaltjänstdirektivet föreskrivs att det i detta direktiv fastställs hur medlemsstaterna ska skilja mellan följande kategorier av betaltjänstleverantörer:
a) Kreditinstitut enligt definitionen i artikel 4.1.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013, inbegripet filialer till dessa enligt definitionen i artikel 4.1.17 i den förordningen, när dessa filialer är belägna

Betaltjänstanvändare: en fysisk eller en juridisk person som utnyttjar en betaltjänst i egenskap av betalare, betalningsmottagare eller båda.

Personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras i synnerhet genom hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Inbyggt dataskydd: tekniska och organisatoriska åtgärder som ingår i en produkt eller tjänst, vilka är utformade för ett effektivt genomförande av dataskyddsprinciper och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas.

Dataskydd som standard: lämpliga tekniska och organisatoriska åtgärder som är genomförda i en produkt eller tjänst för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.

Tekniska tillsynsstandarder: kommissionens delegerade förordning (EU) 2018/389 av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder.

Tredjepartsleverantörer: både leverantörer av betalningsinitieringstjänster och kontoinformationstjänster.

1.2 Tjänster enligt andra betaltjänstdirektivet

5. I andra betaltjänstdirektivet införs två nya typer av betaltjänst(leverantörer), leverantörer av betalningsinitieringstjänster och kontoinformationstjänster. Bilaga 1 till andra betaltjänstdirektivet innehåller åtta betaltjänster som omfattas av direktivet.

6. Leverantörer av betalningsinitieringstjänster tillhandahåller tjänster för att initiera betalningsorder på betaltjänstanvändarens begäran med avseende på ett betalkonto som användaren innehar hos en annan betaltjänstleverantör[11]. En leverantör av betalningsinitieringstjänster kan begära att en kontoförvaltande betaltjänstleverantör (vanligen en

inom unionen, antingen huvudkontoret för de filialerna är belägna inom unionen eller, i enlighet med artikel 47 i direktiv 2013/36/EU och med nationell rätt, utanför unionen.
b) Institut för elektroniska pengar enligt definitionen i artikel 2.1 i direktiv 2009/110/EG, inbegripet, i enlighet med artikel 8 i det direktivet och med nationell rätt, filialer till dessa när dessa filialer är belägna inom unionen och deras huvudkontor är belägna utanför unionen, i den mån de betaltjänster som tillhandahålls av dessa filialer är knutna till utgivning av elektroniska pengar.
c) Postgiroinstitut som enligt nationell rätt har rätt att tillhandahålla betaltjänster.
d) Betalningsinstitut.
e) ECB och nationella centralbanker, när de inte agerar i egenskap av monetär myndighet eller andra offentliga myndigheter.
f) Medlemsstaterna eller deras regionala eller lokala myndigheter, när de inte agerar i egenskap av offentliga myndigheter.

[11] Artikel 4.15 i andra betaltjänstdirektivet.

bank) initierar en transaktion för betaltjänstanvändarens räkning. (Betaltjänst)användaren kan vara en fysisk person (registrerad) eller en juridisk person.

7. Leverantörer av kontoinformationstjänster tillhandahåller onlinetjänster för sammanställd information om ett eller flera betalkonton som betaltjänstanvändaren innehar hos antingen en annan betaltjänstleverantör eller hos fler än en betaltjänstleverantör[12]. Enligt skäl 28 i andra betaltjänstdirektivet ska betaltjänstanvändaren ha möjlighet att omedelbart vid en viss tidpunkt få överblick över sin ekonomiska situation.

8. I fråga om kontoinformationstjänster kan flera olika sorters tjänster erbjudas, med tyngdpunkt på olika särdrag och syften. Vissa leverantörer kan till exempel erbjuda användarna tjänster såsom budgetplanering och övervakning av utgifter. Andra betaltjänstdirektivet är tillämpligt på behandling av personuppgifter i samband med dessa tjänster. Direktivet är inte tillämpligt på tjänster som omfattar kreditbedömningar av betaltjänstanvändaren eller revisionstjänster som genomförs på grundval av en insamling av information via en kontoinformationstjänst och dessa tjänster omfattas därför av dataskyddsförordningen. Vidare är andra betaltjänstdirektivet inte heller tillämpligt på andra konton än betalkonton (t.ex. sparande och investeringar). Dataskyddsförordningen utgör under alla omständigheter den tillämpliga rättsliga ramen för behandlingen av personuppgifter.

Exempel 1:

HappyPayments är ett företag som erbjuder en onlinetjänst som omfattar tillhandahållande av information om ett eller flera betalkonton genom en mobilapp för att tillhandahålla en ekonomisk överblick (en kontoinformationstjänst). Med denna tjänst kan betaltjänstanvändaren få en överblick över saldon och nyligen genomförda transaktioner i två eller flera betalkonton hos olika banker. Om betaltjänstanvändaren väljer det, erbjuder företaget också en kategorisering av utgifter och inkomster i olika kategorier (lön, fritid, energi, bolån osv.) och hjälper således betaltjänstanvändaren med dennes ekonomiska planering. I denna app erbjuder HappyPayments även en tjänst för att initiera betalningar direkt från användarnas betecknade betalningskonto(n) (en betalningsinitieringstjänst).

9. För att dessa tjänster ska kunna tillhandahållas regleras de rättsliga villkor på vilka leverantörer av betalningsinitieringstjänster och kontoinformationstjänster kan få tillgång till betalkonton för att tillhandahålla en tjänst till betaltjänstanvändaren i andra betaltjänstdirektivet.

10. I artiklarna 66.1 och 67.1 i andra betaltjänstdirektivet föreskrivs att betaltjänstanvändaren har rätt till tillgång till och användning av betalnings- och kontoinformationstjänster. Detta innebär att det bör stå betaltjänstanvändaren helt fritt att utöva en sådan rättighet och att denne inte kan tvingas att använda denna rättighet.

11. Tillgång till betalkonton och användning av betalkontoinformation regleras delvis i artiklarna 66 och 67 i andra betaltjänstdirektivet, vilket innehåller skyddsåtgärder för skydd av (person)uppgifter. I artikel 66.3 f i andra betaltjänstdirektivet anges att leverantörer av betalningsinitieringstjänster inte får begära andra uppgifter av betaltjänstanvändaren än sådana som krävs för att tillhandahålla betalningsinitieringstjänsten och i artikel 66.3 g i direktivet föreskrivs att leverantörer av betalningsinitieringstjänster inte får använda, ha tillgång till eller lagra uppgifter för andra ändamål än för att tillhandahålla den betalningsinitieringstjänst som uttryckligen begärs av betaltjänstanvändaren. Enligt artikel 67.2 d i andra betaltjänstdirektivet ska

[12] Artikel 4.16 i andra betaltjänstdirektivet.

vidare leverantörer av kontoinformationstjänster endast ha tillgång till information från betecknade betalkonton och dithörande betalningstransaktionen, medan det i artikel 67.2 f i direktivet föreskrivs att leverantörer av kontoinformationstjänster inte får använda, ha tillgång till eller lagra några uppgifter för några andra ändamål än för att genomföra den kontoinformationstjänst som betaltjänstanvändaren uttryckligen har begärt, i enlighet med uppgiftsskyddsreglerna om uppgiftsskydd. I dessa regler framhålls att personuppgifter endast kan samlas in för särskilda, uttryckligt angivna och berättigade ändamål inom ramen för kontoinformationstjänster. En leverantör av kontoinformationstjänster bör därför uttryckligen ange i avtalet för vilka särskilda ändamål personliga kontoinformationsuppgifter kommer att behandlas i samband med de kontoinformationstjänster denne tillhandahåller. Enligt artikel 5 i dataskyddsförordningen ska avtalet vara lagligt, korrekt och öppet samt vidare även följa annan konsumentlagstiftning.

12. Beroende på särskilda omständigheter kan betaltjänstleverantörer utgöra personuppgiftsansvariga eller personuppgiftsbiträden enligt dataskyddsförordningen. I dessa riktlinjer är de betaltjänstleverantörer som, själva eller tillsammans med andra, fastställer ändamålen med och medlen för behandlingen av personuppgifter personuppgiftsansvariga. Mer vägledning om detta finns i dataskyddsstyrelsens riktlinjer 07/2020 om begreppen personuppgiftsansvarig och personuppgiftsbiträde enligt dataskyddsförordningen.

2 LAGLIGA GRUNDER OCH YTTERLIGARE BEHANDLING ENLIGT ANDRA BETALTJÄNSTDIREKTIVET

2.1 Lagliga grunder för behandling

13. Enligt dataskyddsförordningen ska personuppgiftsansvariga ha en rättslig grund för att behandla personuppgifter. Artikel 6.1 i dataskyddsförordningen innehåller en uttömmande och begränsande förteckning över sex rättsliga grunder för behandling av personuppgifter enligt dataskyddsförordningen[13]. Det ankommer på den personuppgiftsansvarige att definiera den lämpliga rättsliga grunden och säkerställa att samtliga villkor är uppfyllda. Avgörande för fastställandet vilken grund som är giltig och mest lämplig i en särskild situation är de omständigheter under vilka behandlingen äger rum, inbegripet ändamålet med behandlingen och förhållandet mellan den personuppgiftsansvarige och den registrerade.

2.2 Artikel 6.1 b i dataskyddsförordningen (behandlingen är nödvändig för att fullgöra ett avtal)

14. Betalningstjänster tillhandahålls på grund av ett avtal mellan betaltjänstanvändaren och betaltjänstleverantören. I skäl 87 i andra betaltjänstdirektivet anges ”[d]etta direktiv bör endast gälla skyldigheter och ansvar enligt avtalet mellan betaltjänstanvändaren och dennes betaltjänstleverantör.” När det gäller dataskyddsförordningen utgör den huvudsakliga rättsliga grunden för behandling av personuppgifter för tillhandahållande av betalningstjänster artikel 6.1 b i dataskyddsförordningen, vilket innebär att behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

15. Betalningstjänsterna enligt andra betaltjänstdirektivet definieras i bilaga 1 till nämnda direktiv. Tillhandahållandet av dessa tjänster såsom de definieras enligt andra betaltjänstdirektivet utgör ett villkor för att det ska uppkomma ett avtal enligt vilket parterna har tillgång till betaltjänstanvändarens betalkontouppgifter. Dessa betaltjänstleverantörer ska även vara auktoriserade aktörer. I förhållande till betalningsinitieringstjänster och kontoinformationstjänster enligt andra betaltjänstdirektivet kan avtal även innehålla villkor om

[13] Enligt artikel 6 är behandlingen endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllda:

(a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

(b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

(c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

(d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

(e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

(f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

ytterligare tjänster som inte är reglerade i andra betaltjänstdirektivet. I dataskyddsstyrelsens riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, klargörs att personuppgiftsansvariga ska bedöma vilken behandling av personuppgifter som objektivt sett är nödvändig för fullgörandet av avtalet. I dessa riktlinjer påpekas att frågan huruvida behandlingen är nödvändig beror på vad för slags tjänst det är frågan om, avtalsparternas ömsesidiga perspektiv och förväntningar, avtalets logiska grund och avtalets grundsatser.

16. I dataskyddsstyrelsens riktlinjer 2/2019 klargörs även att det, mot bakgrund av artikel 7.4 i dataskyddsförordningen, görs skillnad mellan behandling som är nödvändig för fullgörandet av ett avtal och klausuler som gör tjänsten beroende av viss behandlingsverksamhet som i själva verket inte är nödvändig för avtalets fullgörande. ”Nödvändig för fullgörandet” kräver helt klart något utöver ett avtalsvillkor[14]. Den personuppgiftsansvarige bör kunna visa hur huvudföremålet i det angivna avtalet med den registrerade rent faktiskt inte kan fullgöras om den särskilda behandlingen av personuppgifterna i fråga inte äger rum. Att endast hänvisa till eller nämna uppgiftsbehandling i ett avtal räcker inte för att behandlingen i fråga ska omfattas av artikel 6.1 b i dataskyddsförordningen.

17. I artikel 5.1 b i dataskyddsförordningen fastställs principen om ändamålsbegränsning, enligt vilken det krävs att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. När man bedömer om artikel 6.1 b är en lämplig rättslig behandlingsgrund i samband med en (betal)tjänst online, bör man ta hänsyn till tjänstens särskilda mål, syfte eller ändamål[15]. Ändamålen med behandlingen måste anges tydligt och meddelas till den registrerade i enlighet med den personuppgiftsansvariges ändamålsbegränsnings- och öppenhetsskyldigheter. Att bedöma vad som är ”nödvändigt” innebär en kombinerad, faktabaserad bedömning av behandlingen ”för det mål som åsyftas och av huruvida det är mindre integritetskränkande jämfört med andra alternativ för hur man uppnår samma mål”. Artikel 6.1 b omfattar inte behandling som är användbar men objektivt sett inte nödvändig för att utföra den avtalade tjänsten eller för att vidta de relevanta avtalsförberedande åtgärderna på den registrerades begäran, även om det är nödvändigt för den personuppgiftsansvariges andra verksamhetsändamål[16].

18. I dataskyddsstyrelsens riktlinjer 2/2019 klargörs att ett avtal inte på konstlad väg kan utöka kategorierna av personuppgifter eller de typer av behandling som den personuppgiftsansvarige måste utföra för fullgörandet av avtalet i den mening som avses i artikel 6.1 b[17]. I riktlinjerna behandlas även fall i vilka en ”allt eller inget”-situation kan uppkomma för registrerade som kanske endast är intresserade av en av tjänsterna. Detta kan hända om en personuppgiftsansvarig vill skapa ett paket av flera fristående tjänster eller delar av en tjänst med olika grundläggande ändamål, kännetecken eller motivering i ett enda avtal. Om ett avtal består av flera fristående tjänster eller delar av en tjänst som i själva verket rimligen kan utföras oberoende av varandra bör tillämpningen av artikel 6.1 b bedömas mot bakgrund av var och en av dessa tjänster separat, genom att man tittar på vad som objektivt sett är nödvändigt för att utföra var och en av de enskilda tjänster som den registrerade aktivt har begärt eller anmält sig till[18].

[14] Dataskyddsstyrelsens riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, sidan 8.
[15] Ibid.
[16] Ibid, sidan 7.
[17] Ibid, sidan 10.
[18] Ibid, sidan 11.

19. I överensstämmelse med ovannämnda riktlinjer har personuppgiftsansvariga en skyldighet att bedöma vad som objektivt sett är nödvändigt för fullgörandet av avtalet. Om personuppgiftsansvariga inte kan visa att behandlingen av de personliga betalkontouppgifterna inte objektivt sett är nödvändig för tillhandahållandet av var och en av dessa tjänster separat, utgör artikel 6.1 b i dataskyddsförordningen inte en giltig rättslig grund för behandlingen. I dessa situationer bör den personuppgiftsansvarige överväga en annan rättslig grund för behandlingen.

2.3 Förebyggande av bedrägerier

20. I artikel 94.1 i andra betaltjänstdirektivet föreskrivs att medlemsstaterna ska tillåta att betalningssystem och betaltjänstleverantörer behandlar personuppgifter när det är nödvändigt för att säkerställa förebyggande, undersökning och avslöjande av betalningsbedrägerier. Sådan behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier kan utgöra ett berättigat intresse för den berörda betaltjänstleverantören, under förutsättning att den registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre än betaltjänstleverantörens intressen[19]. Behandling för att förhindra bedrägerier skulle kunna grundas på en noggrann bedömning från den personuppgiftsansvarige i varje enskilt fall, i enlighet med ansvarsprincipen. För att förhindra bedrägerier kan personuppgiftsansvariga även omfattas av särskilda rättsliga förpliktelser som gör att en behandling av personuppgifter är nödvändig.

2.4 Ytterligare behandling (leverantörer av kontoinformationstjänster och betalningsinitieringstjänster)

21. I artikel 6.4 i dataskyddsförordningen fastställs villkoren för behandling av personuppgifter för andra ändamål än det ändamål för vilket personuppgifterna samlades in. Mer konkret får sådan ytterligare behandling genomföras som grundar sig på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att säkerställa de mål som avses i artikel 23.1, där den registrerade har lämnat sitt samtycke eller om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in är förenligt med det ursprungliga ändamålet.

22. Artiklarna 66.3 g och 67.2 f i andra betaltjänstdirektivet måste beaktas noga. Såsom angetts ovan anges det i artikel 66.3 g i andra betaltjänstdirektivet att leverantörer av betalningsinitieringstjänster inte får använda, ha tillgång till eller lagra uppgifter för andra ändamål än för att tillhandahålla den betalningsinitieringstjänst som uttryckligen begärs av betalaren. I artikel 67.2 f i andra betaltjänstdirektivet anges att leverantörer av kontoinformationstjänster inte får använda, ha tillgång till eller lagra några uppgifter för några andra ändamål än för att genomföra den kontoinformationstjänst som betaltjänstanvändaren uttryckligen har begärt, i enlighet med uppgiftsskyddsreglerna om uppgiftsskydd.

23. Genom artiklarna 66.3 g och 67.2 f i andra betaltjänstdirektivet begränsas följaktligen möjligheterna till behandling för andra ändamål avsevärt, vilket innebär behandling för andra ändamål endast är tillåten om den registrerade har lämnat samtycke enligt artikel 6.1 a i dataskyddsförordningen eller behandlingen föreskrivs i unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av enligt artikel 6.4 i dataskyddsförordningen. Om behandlingen för andra ändamål än det ändamål för vilket personuppgifterna samlades inte grundas på den registrerades samtycke eller unionsrätten eller medlemsstaternas nationella rätt, framgår det av de begränsningar som föreskrivs i artiklarna 66.3 g och 67.2 f i andra betaltjänstdirektivet att andra ändamål inte är förenliga med det ändamål för

[19] Skäl 47 i dataskyddsförordningen.

vilket personuppgifterna ursprungligen samlades in. Den förenlighetsbedömning som föreskrivs i artikel 6.4 i dataskyddsförordningen kan inte utgöra rättslig grund för behandlingen.

24. Enligt artikel 6.4 i dataskyddsförordningen medges ytterligare behandling som grundar sig på unionsrätten eller medlemsstaternas nationella rätt. Exempelvis utgör alla leverantörer av betalningsinitieringstjänster och kontoinformationstjänster ansvariga enheter enligt artikel 3.2 a i Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism (penningtvättsdirektivet). Dessa ansvariga enheter är därför skyldiga att tillämpa de åtgärder för kundkännedom som anges i detta direktiv. De personuppgifter som behandlas i samband med en tjänst enligt andra betaltjänstdirektivet behandlas därför ytterligare på grundval av minst en rättslig förpliktelse som åligger tjänsteleverantören[20].

25. Såsom anges i punkt 20 framgår det av artikel 6.4 i dataskyddsförordningen att behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in kan grundas på den registrerades samtycke, om samtliga villkor för samtycke enligt dataskyddsförordningen är uppfyllda. Såsom anges ovan måste den personuppgiftsansvarige visa att det är möjligt att utan problem vägra eller ta tillbaka sitt samtycke (skäl 42 i dataskyddsförordningen).

2.5 Laglig grund för att bevilja tillgång till kontot (kontoförvaltande betaltjänstleverantörer)

26. Såsom anges i punkt 10 kan betaltjänstanvändare utöva sin rätt att använda betalningsinitiering och kontoinformationstjänster. De skyldigheter som medlemsstaterna åläggs i artiklarna 66.1 och 67.1 i andra betaltjänstdirektivet bör införlivas i nationell rätt för att garantera en effektiv tillämpning av betaltjänstanvändarens rätt att dra nytta av ovannämnda betaltjänster. Om den kontoförvaltande betaltjänstleverantören, normalt sett en bank, inte har någon motsvarande skyldighet att bevilja betaltjänstleverantören tillgång till kontot, under förutsättning att denne uppfyller alla krav för att erhålla tillgång till betaltjänstanvändarens konto, är en effektiv tillämpning av sådana rättigheter inte möjlig. Vidare anges det tydligt i artiklarna 66.5 och 67.4 i andra betaltjänstdirektivet att tillhandahållandet av betalningsinitieringstjänster och kontoinformationstjänster inte får vara avhängigt av förekomsten av ett avtalsförhållande mellan leverantören av betalningsinitieringstjänster eller kontoinformationstjänster och den kontoförvaltande betaltjänstleverantören.

27. Den kontoförvaltande betaltjänstleverantörens behandling av personuppgifter, vilken består av att bevilja tillgång till de personuppgifter som leverantören av betalningsinitieringstjänster eller kontoinformationstjänster begär för att fullgöra sin betaltjänst till betaltjänstanvändaren, grundas på en rättslig förpliktelse. För att uppnå målen i andra betaltjänstdirektivet måste kontoförvaltande betaltjänstleverantörer tillhandahålla personuppgifterna för tjänsterna från leverantörerna av betalningsinitieringstjänster och kontoinformationstjänster, vilket utgör en nödvändig förutsättning för att dessa ska kunna tillhandahålla sina tjänster, och därigenom garantera de rättigheter som föreskrivs i artiklarna 66.1 och 67.1 i andra betaltjänstdirektivet. Den tillämpliga rättsliga grunden i sådana fall är därför artikel 6.1 c i dataskyddsförordningen.

28. Eftersom det anges i dataskyddsförordningen att behandling som grundas på en rättslig förpliktelse tydligt ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt (se artikel 6.3 i dataskyddsförordningen), ska skyldigheten för kontoförvaltande

[20] Notera att detta dokument inte omfattar någon grundlig undersökning av frågan huruvida penningtvättsdirektivet uppfyller kraven i artikel 6.4 i dataskyddsförordningen.

betaltjänstleverantörer att bevilja tillgång följa av den nationella lagstiftning genom vilken andra betaltjänstdirektivet har införlivats.

3 UTTRYCKLIGT SAMTYCKE

3.1 Samtycke enligt dataskyddsförordningen

29. Enligt dataskyddsförordningen utgör samtycke en av de sex rättsliga grunderna för laglig behandling av personuppgifter. Enligt artikel 4.11 i dataskyddsförordningen definieras samtycke som ”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”. För att samtycket ska vara giltigt är det avgörande att dessa fyra villkor är uppfyllda, nämligen att samtycket är frivilligt, specifikt, informerat och otvetydigt. Enligt dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679 kan samtycke enbart vara den lämpliga rättsliga grunden om den registrerade erbjuds kontroll och får en genuin valmöjlighet att godta eller vägra godta de villkor som ges eller att vägra godta dem utan problem. När den personuppgiftsansvarige ber om samtycke måste han eller hon bedöma huruvida samtliga villkor kommer att uppfyllas för erhållandet av giltigt samtycke. Om samtycke erhålls helt i linje med den allmänna dataskyddsförordningen är samtycke ett verktyg som ger de registrerade kontroll över huruvida deras personuppgifter kommer att behandlas. I annat fall blir de registrerades kontroll skenbar och samtycke kommer då att vara en ogiltig rättslig grund för behandling, vilket innebär att behandlingen blir olaglig[21].

30. Dataskyddsförordningen innehåller även ytterligare skyddsåtgärder i artikel 7, där det föreskrivs att den personuppgiftsansvarige ska kunna visa att det förelåg giltigt samtycke vid tidpunkten för behandlingen. Begäran om samtycke ska även läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Vidare ska den registrerade informeras om rätten att när som helst återkalla samtycket lika enkelt som att lämna samtycke.

31. Enligt artikel 9 i dataskyddsförordningen utgör samtycke ett av undantagen från det allmänna förbudet att behandla särskilda kategorier av personuppgifter. I sådana situationer krävs det emellertid att den registrerade ”uttryckligen” lämnat samtycke[22].

32. Enligt dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679 avses med uttryckligt samtycke enligt dataskyddsförordningen hur den registrerade lämnar sitt samtycke. Det innebär att den registrerade måste avge en uttrycklig samtyckesförklaring för behandling för särskilda ändamål. Ett självklart sätt att se till att samtycket är uttryckligt är att uttryckligen bekräfta sitt samtycke i en skriftlig förklaring. Där så är lämpligt skulle den personuppgiftsansvarige kunna säkerställa att den skriftliga förklaringen undertecknas av den registrerade, för att undanröja alla eventuella tvivel och risker för bristande bevisning i framtiden.

33. Under inga omständigheter kan samtycke erhållas genom potentiellt tvetydiga förklaringar eller handlingar. En personuppgiftsansvarig måste också vara medveten om att samtycke inte får erhållas genom att den registrerade godtar ett avtal eller allmänna villkor för en viss tjänst.

3.2 Samtycke enligt andra betaltjänstdirektivet

[21] Dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/ 679, punkt 3.
[22] Se även yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), s. 6–8, och/eller yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG (WP 217), s. 9, 10, 13 och 14.

34. Styrelsen noterar att den rättsliga ramen för uttryckligt samtycke är komplex, eftersom både andra betaltjänstdirektivet och dataskyddsförordningen innehåller begreppet ”uttryckligt samtycke”. Detta leder fram till frågan huruvida ”uttryckligt medgivande” såsom anges i artikel 94.2 i andra betaltjänstdirektivet bör tolkas på samma sätt som uttryckligt samtycke enligt dataskyddsförordningen.

3.2.1 Uttryckligt medgivande enligt artikel 94.2 i andra betaltjänstdirektivet

35. Andra betaltjänstdirektivet innehåller ett antal särskilda bestämmelser som rör behandling av personuppgifter, särskilt artikel 94.1 i direktivet, där det fastställs att behandling av personuppgifter enligt andra betaltjänstdirektivet måste följa EU:s dataskyddslagstiftning. Vidare föreskrivs det i artikel 94.2 i andra betaltjänstdirektivet att betaltjänstleverantörer endast ska ha tillgång till, behandla och bevara sådana personuppgifter som är nödvändiga för tillhandahållande av betaltjänsterna, med uttryckligt medgivande från betaltjänstanvändaren. Enligt artikel 33.2 i andra betaltjänstdirektivet är detta krav på uttryckligt medgivande från betaltjänstanvändaren inte tillämpligt på leverantörer av kontoinformationstjänster. Emellertid föreskrivs uttryckligt godkännande för leverantörer av kontoinformationstjänster för tillhandahållandet av tjänsten enligt artikel 67.2 a i andra betaltjänstdirektivet.

36. Såsom angetts ovan är förteckningen över grunder för laglig behandling i dataskyddsförordningen uttömmande. Såsom anges i punkt 14 utgör i princip artikel 6.1 b i dataskyddsförordningen den rättsliga grunden för behandling av personuppgifter för tillhandahållande av betaltjänster, vilket innebär att behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Av detta följer att artikel 94.2 i andra betaltjänstdirektivet inte kan betraktas som en ytterligare rättslig grund för behandling av personuppgifter. Mot denna bakgrund anser styrelsen att denna bestämmelse dels ska tolkas i enlighet med den tillämpliga rättsliga ramen för dataskydd och dels på ett sådant sätt att dess ändamålsenliga verkan bibehålls. Uttryckligt medgivande enligt artikel 94.2 i andra betaltjänstdirektivet ska därför betraktas som ett ytterligare avtalsrättsligt krav[23] i förhållande till tillgång till och efterföljande behandling och lagring av personuppgifter för att tillhandahålla betaltjänster och har därför inte samma innebörd som (uttryckligt) samtycke enligt dataskyddsförordningen.

37. ”Uttryckligt medgivande” till vilket hänvisas i artikel 94.2 i andra betaltjänstdirektivet utgör ett samtycke genom avtal. Detta innebär att artikel 94.2 i andra betaltjänstdirektivet bör tolkas så, att registrerade när de ingår ett avtal med en betaltjänstleverantör enligt andra betaltjänstdirektivet måste få full kännedom om vilka särskilda kategorier av personuppgifter som kommer att behandlas. Vidare ska de få kännedom om det särskilda ändamål (för betaltjänster) för vilket deras personuppgifter kommer att behandlas och uttryckligen godkänna dessa klausuler. Sådana klausuler bör klart och tydligt kunna särskiljas från de andra frågor som behandlas i avtalet och det krävs att den registrerade uttryckligen godtar dem.

38. Erhållandet av tillgång till personuppgifter för efterföljande behandling och lagring av dessa uppgifter i syfte att tillhandahålla betaltjänster har central betydelse för begreppet ”uttryckligt medgivande” enligt artikel 94.2 i andra betaltjänstdirektivet. Detta innebär att betaltjänstleverantören[24] ännu inte behandlar personuppgifterna, utan behöver tillgång till personuppgifter som har behandlats under ansvar av någon annan personuppgiftsansvarig. Om en betaltjänstanvändare ingår ett avtal med, till exempel, en leverantör av en

[23] Dataskyddsstyrelsens skrivelse om andra betaltjänstdirektivet, 5 juli 2018, sidan 4.
[24] Detta är tillämpligt på tjänsterna 1–7 i bilaga 1 till andra betaltjänstdirektivet.

betalningsinitieringstjänst, behöver denna leverantör erhålla tillgång till personuppgifter från betaltjänstanvändaren som behandlas under den kontoförvaltande betaltjänstleverantörens ansvar. Syftet med det uttryckliga medgivandet enligt artikel 94.2 i andra betaltjänstdirektivet är att erhålla tillgång till dessa personuppgifter för att kunna behandla och lagra de personuppgifter som är nödvändiga för att kunna tillhandahålla betaltjänsten. Om den registrerade lämnar uttryckligt medgivande är den kontoförvaltande betaltjänstleverantören skyldig att ge tillgång till de angivna personuppgifterna.

39. Även om medgivandet enligt artikel 94.2 i andra betaltjänstdirektivet inte utgör en rättslig grund för behandling av personuppgifter, hänför sig detta medgivande särskilt till personuppgifter och dataskydd och garanterar öppenhet och en viss kontroll för betaltjänstanvändaren[25]. Medan de materiella villkoren för medgivande enligt artikel 94.2 i andra betaltjänstdirektivet inte anges i direktivet, bör det, såsom anges ovan, tolkas i överensstämmelse med den tillämpliga rättsliga ramen för dataskydd samt så att dess ändamålsenliga verkan bibehålls.

40. Vad gäller den information som personuppgiftsansvariga ska tillhandahålla och kravet på öppenhet anges i artikel 29-gruppens riktlinjer om öppenhet ”[e]n viktig aspekt av den öppenhetsprincip som beskrivs i dessa bestämmelser är att de registrerade på förhand bör kunna avgöra syftet med och konsekvenserna av behandlingen och att det inte bör komma som en överraskning för dem i ett senare skede hur deras personuppgifter har använts”[26].

41. Personuppgifter ska vidare, i enlighet med principen om ändamålsbegränsning, samlas in för särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b i dataskyddsförordningen). Om personuppgifter samlas in för mer än ett ändamål *bör personuppgiftsansvariga undvika att endast identifiera ett brett ändamål för att motivera olika former av ytterligare behandling som i själva verket enbart har ett avlägset samband med det faktiska ursprungliga ändamålet*[27]. Senast i samband med avtal för nättjänster har styrelsen framhållit risken för att inkludera allmänna behandlingsvillkor i avtal och har angett att syftet med insamlingen måste anges tydligt och specifikt. Det måste vara tillräckligt detaljerat för att fastställa vilken typ av behandling som inbegrips och inte inbegrips i det angivna syftet, och möjliggöra att efterlevnaden av lagen kan bedömas och uppgiftsskyddsgarantierna kan tillämpas[28].

42. Mot bakgrund av det ytterligare kravet på uttryckligt medgivande enligt artikel 94.2 i andra betaltjänstdirektivet, innebär detta att personuppgiftsansvariga måste ge de registrerade särskild och specifik information om de särskilda ändamål som den personuppgiftsansvarige har identifierat, för vilka deras personuppgifter hämtas, behandlas och lagras. I överensstämmelse med artikel 94.2 i andra betaltjänstdirektivet måste registrerade uttryckligen godta dessa särskilda ändamål.

43. Såsom anges ovan i punkt 10 framhåller styrelsen dessutom att betaltjänstanvändaren måste kunna välja om denne vill använda tjänsten eller inte och kan inte tvingas att göra detta. Därför måste medgivandet enligt artikel 94.2 i andra betaltjänstdirektivet även ges frivilligt.

3.3 Slutsats

[25] Artikel 94.2 i andra betaltjänstdirektivet omfattas av kapitel 4 ”dataskydd”.
[26] Artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679, punkt 10 (antagna den 11 april 2018) som godkänts av dataskyddsstyrelsen.
[27] Artikel 29-gruppens yttrande 03/2013 om ändamålsbegränsning (WP203), sidan 16.
[28] Riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, punkt 16 (version för offentligt samråd) och artikel 29-gruppens yttrande 03/2013 om ändamålsbegränsning (WP203), sidorna 15–16.

44. Uttryckligt medgivande enligt andra betaltjänstdirektivet skiljer sig från (uttryckligt) samtycke enligt dataskyddsförordningen. Uttryckligt medgivande enligt artikel 94.2 i andra betaltjänstdirektivet utgör ett ytterligare krav av avtalsrättslig karaktär. Om en betaltjänstleverantör behöver tillgång till personuppgifter för tillhandahållandet av en betaltjänst krävs det uttryckligt medgivande från betaltjänstanvändaren i enlighet med artikel 94.2 i andra betaltjänstdirektivet.

4 BEHANDLING AV UPPGIFTER FRÅN PASSIVA PARTER

4.1 Uppgifter från passiva parter

45. En fråga som rör uppgiftsskydd som måste övervägas noga är behandling av uppgifter från så kallade ”passiva parter”. Inom ramen för detta dokument utgör uppgifter från passiva parter personuppgifter från en registrerad som inte använder en särskild betaltjänstleverantör, men vars personuppgifter behandlas av denna särskilda betaltjänstleverantör för att fullgöra ett avtal mellan leverantören och betaltjänstanvändaren. Detta är exempelvis fallet om en betaltjänstanvändare, registrerad A, använder tjänster från en leverantör av kontotjänster och registrerad B har gjort ett antal betalningstransaktioner till A:s betalkonto. I denna situation betraktas B som den ”passiva parten” och de personuppgifter (såsom B:s kontonummer och det belopp som dessa transaktioner omfattade) som rör B betraktas som ”uppgifter från passiva parter”.

4.2 Den personuppgiftsansvariges berättigade intresse

46. Enligt artikel 5.1 b i dataskyddsförordningen krävs det att personuppgifter endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. I dataskyddsförordningen uppställs även krav på att all behandling av personuppgifter måste vara både nödvändig och proportionerlig samt överensstämma med principerna för dataskydd, såsom principerna om ändamålsbegränsning och uppgiftsminimering.

47. Behandling av uppgifter från passiva parter kan vara tillåten enligt dataskyddsförordningen om behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen (artikel 6.1 f i dataskyddsförordningen). Sådan behandling är emellertid endast tillåten såvida inte ”den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre” än den personuppgiftsansvariges berättigade intressen och kräver skydd av personuppgifter.

48. I samband med tillhandahållande av betaltjänster enligt andra betaltjänstdirektivet skulle en laglig grund för behandling av uppgifter från passiva parter från leverantörer av betalningsinitieringstjänster och kontoinformationstjänster således kunna vara den personuppgiftsansvariges eller en tredje parts berättigade intressen att fullgöra avtalet med betaltjänstanvändaren. Behovet av att behandla personuppgifter från den passiva parten är begränsat till och bestäms av dessa registrerades rimliga förväntningar. I samband med tillhandahållandet av betaltjänster som omfattas av andra betaltjänstdirektivet ska effektiva och lämpliga åtgärder fastställas för att säkerställa att passiva parters intressen eller grundläggande rättigheter och friheter inte åsidosätts och att dessa registrerades rimliga förväntningar vad gäller behandlingen av deras personuppgifter respekteras. I detta hänseende krävs det att den personuppgiftsansvarige (en leverantör av kontoinformationstjänster eller betalningsinitieringstjänster) vidtar de skyddsåtgärder som är nödvändiga för behandlingen för att skydda de registrerades intressen. Detta omfattar tekniska åtgärder för att säkerställa att uppgifter från passiva parter inte behandlas för andra ändamål än det ändamål för vilket leverantörerna av betalningsinitieringstjänster och kontoinformationstjänster ursprungligen samlade in personuppgifterna. Om det är möjligt ska även kryptering eller annan teknik användas för att åstadkomma en lämplig nivå vad gäller säkerhet och uppgiftsminimering.

4.3 Ytterligare behandling av personuppgifter från den passiva parten

49. Såsom anges i punkt 29 kan personuppgifter som behandlas i samband med en betalningstjänst som regleras i andra betaltjänstdirektivet behandlas ytterligare på grundval av rättsliga

förpliktelser som åvilar tjänsteleverantören. Dessa rättsliga förpliktelser kan röra personuppgifter från den passiva parten.

50. Vad gäller ytterligare behandling av uppgifter från passiva parter på grundval av berättigade intressen, anser styrelsen att dessa uppgifter inte kan användas för ett annat ändamål än det för vilket personuppgifterna samlades in, förutom på grundval av EU-rätten eller medlemsstaternas nationella rätt. I rättsligt hänseende är det inte möjligt att inhämta samtycke från den passiva parten, eftersom dennes personuppgifter behöver samlas in eller behandlas för att erhålla samtycke, för vilket det inte finns någon rättslig grund enligt artikel 6 i dataskyddsförordningen. Inte heller kan den förenlighetsbedömning som föreskrivs i artikel 6.4 i dataskyddsförordningen utgöra en grund för behandling för andra ändamål (t.ex. direktmarknadsföring). Dessa registrerade passiva parters rättigheter och friheter respekteras inte om en ny personuppgiftsansvarig använder personuppgifterna för andra ändamål, med beaktande av det sammanhang inom vilket personuppgifterna har samlats in, särskilt eftersom det inte finns något förhållande till de registrerade som är passiva parter[29], avsaknaden av samband mellan något annat ändamål och det ändamål för vilket personuppgifterna ursprungligen samlades in (dvs. det faktum att betaltjänstleverantörer endast behöver den passiva partens uppgifter för att fullgöra ett avtal med den andra avtalsparten), de berörda personuppgifternas art[30], det förhållandet att registrerade inte rimligen kan förvänta sig ytterligare behandling eller vara medvetna om vilken personuppgiftsansvarig som kan komma att behandla deras personuppgifter och mot bakgrund av de rättsliga begränsningar av behandlingen som föreskrivs i artikel 66.3 g och artikel 67.2 f i andra betaltjänstdirektivet.

[29] I skäl 87 i andra betaltjänstdirektivet anges att direktivet endast gäller ”skyldigheter och ansvar enligt avtalet mellan betaltjänstanvändaren och dennes betaltjänstleverantör”. Andra betaltjänstdirektivet är därför inte tillämpligt på uppgifter från passiva parter.

[30] Särskild hänsyn ska tas vid behandling av personuppgifter av finansiell karaktär, eftersom behandlingen kan anses öka de eventuella riskerna för enskildas rättigheter och friheter, enligt riktlinjerna om konsekvensbedömning avseende dataskydd.

5 BEHANDLING AV SÄRSKILDA KATEGORIER AV PERSONUPPGIFTER ENLIGT ANDRA BETALTJÄNSTDIREKTIVET

5.1 Särskilda kategorier av personuppgifter

51. Enligt artikel 9.1 i dataskyddsförordningen ska behandling av ”personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning” vara förbjuden.

52. Det bör framhållas att elektroniska betalningar redan är allmänt förekommande i vissa medlemsstater och att många människor föredrar dem framför kontanter vid sina dagliga transaktioner. Samtidigt kan finansiella transaktioner avslöja känslig information om en enskild registrerad, inbegripet sådan som hänför sig till särskilda kategorier av personuppgifter. På grundval av transaktionsuppgifter kan donationer till politiska partier eller organisationer, kyrkor eller församlingar exempelvis avslöja politiska uppfattningar och religiösa övertygelser. Medlemskap i fackförbund kan avslöjas genom att en årlig medlemsavgift dras från en persons bankkonto. Genom analysering av fakturor för sjukvård som en registrerad har betalat till en läkare (t.ex. en psykiater) är det möjligt att samla in personuppgifter som rör hälsa. Slutligen kan information om vissa inköp ge information om en persons sexualliv eller sexuella läggning. Såsom framgår av dessa exempel kan till och med enskilda transaktioner innehålla särskilda kategorier av personuppgifter. Vidare kan kontoinformationstjänster bygga på profilering såsom den definieras i artikel 4.4 i dataskyddsförordningen. Såsom redan angetts i artikel 29-gruppen riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, som godkänts av dataskyddsstyrelsen, kan ”[p]rofilering […] skapa särskilda kategorier av uppgifter genom att dra slutsatser från och kombinera uppgifter som inte utgör en särskild kategori av uppgifter.”[31] Detta innebär att de sammantagna finansiella transaktionerna kan avslöja olika beteendemönster, vilket kan omfatta särskilda kategorier av personuppgifter. Därför är chanserna stora att en tjänsteleverantör som behandlar information om registrerades finansiella transaktioner även behandlar särskilda kategorier av personuppgifter.

53. Vad gäller begreppet ”känsliga betalningsuppgifter” noterar styrelsen följande: Definitionen av känsliga betalningsuppgifter i andra betaltjänstdirektivet skiljer sig avsevärt från hur begreppet ”känsliga personuppgifter” normalt sätt används i samband med dataskyddsförordningen och (lagstiftningen om) uppgiftsskydd. Medan andra betaltjänstdirektivet definierar ”känsliga betalningsuppgifter” som ”uppgifter, inbegripet personliga säkerhetsbehörighetsuppgifter, som kan användas för bedrägerier”, framhävs i dataskyddsförordningen behovet av särskilt skydd för särskilda kategorier av personuppgifter som enligt artikel 9 i dataskyddsförordningen till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter såsom särskilda kategorier av personuppgifter[32]. I detta hänseende rekommenderar styrelsen att det åtminstone ska kartläggas och exakt kategoriseras vilken typ av personuppgifter som kommer att behandlas. Med största sannolikhet krävs det en konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen, vilket kommer att vara till hjälp vid denna kartläggning. Mer vägledning om sådana konsekvensbedömningar finns i artikel 29-gruppens riktlinjer om

[31] Artikel 29-gruppen, riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, WP251, rev.01, s. 15.

[32] I skäl 10 i dataskyddsförordningen hänvisas till särskilda kategorier av personuppgifter som ”känsliga uppgifter”.

konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679 som godkänts av styrelsen.

5.2 Möjliga undantag

54. Förbudet i artikel 9 i dataskyddsförordningen är inte absolut. Medan det är uppenbart att undantagen i artikel 9.2 b–f och h–j i dataskyddsförordningen inte är tillämpliga på behandling av personuppgifter i samband med andra betaltjänstdirektivet, skulle särskilt följande två undantag i artikel 9.2 i dataskyddsförordningen kunna beaktas:

a) Förbudet är inte tillämpligt om den registrerade har lämnat uttryckligt samtycke till behandling av dessa personuppgifter för ett eller flera mer specifika ändamål (artikel 9.2 a i dataskyddsförordningen).

b) Förbudet är inte tillämpligt om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (artikel 9.2 g i dataskyddsförordningen).

55. Det ska påpekas att förteckningen över undantag i artikel 9.2 i dataskyddsförordningen är uttömmande. Tjänsteleverantörer måste räkna med att det är möjligt att särskilda kategorier av personuppgifter ingår i de personuppgifter som behandlas för tillhandahållandet av någon av de tjänster som omfattas av andra betaltjänstdirektivet. Eftersom förbudet enligt artikel 9.1 i dataskyddsförordningen är tillämpligt på dessa tjänsteleverantörer har de en skyldighet att säkerställa att ett av undantagen i artikel 9.2 i dataskyddsförordningen är tillämpligt på dem. Det bör framhållas att förbudet i artikel 9.1 är tillämpligt om tjänsteleverantören inte kan visa att något av undantagen är uppfyllda.

5.3 Viktigt allmänt intresse

56. Betalningstjänster får behandla särskilda kategorier av personuppgifter av hänsyn till ett viktigt allmänt intresse, men detta gäller enbart om samtliga villkor i artikel 9.2 g i dataskyddsförordningen är uppfyllda. Detta innebär att behandlingen av de särskilda kategorierna av personuppgifter ska föreskrivas i ett särskilt undantag till artikel 9.1 i dataskyddsförordningen i unionsrätten eller medlemsstaternas nationella rätt. Proportionaliteten i förhållande till det eftersträvade syftet med behandlingen måste behandlas i denna bestämmelse och den måste innehålla lämpliga och specifika åtgärder för att garantera den registrerades grundläggande rättigheter och intressen. Vidare måste denna unionsrättsliga bestämmelse eller bestämmelse i medlemsstaternas nationella rätt vara förenlig med det centrala innehållet i rätten till dataskydd. Slutligen måste det visas att behandlingen av de särskilda kategorierna av uppgifter är nödvändig av hänsyn till ett viktigt allmänt intresse, inbegripet intressen som har systemviktig betydelse. Undantaget kan endast tillämpas på betecknade typer av betaltjänster om alla dessa villkor är helt uppfyllda.

5.4 Uttryckligt samtycke

57. Det enda möjliga lagliga undantag som återstår för behandling av särskilda kategorier av personuppgifter genom tredjepartsleverantörer i situationer där undantaget enligt artikel 9.2 g i dataskyddsförordningen inte är tillämpligt är att erhålla uttryckligt samtycke i enlighet med villkoren för giltigt samtycke i dataskyddsförordningen. I dataskyddsstyrelsens riktlinjer 05/2020

om samtycke enligt förordning (EU) 2016/679 anges[33] följande: ”[e]nligt artikel 9.2 betraktas inte ’nödvändig för att fullgöra ett avtal’ som ett undantag till det allmänna förbudet mot att behandla särskilda kategorier av uppgifter. Personuppgiftsansvariga och medlemsstater som handskas med sådana situationer bör därför undersöka de särskilda undantagen i artikel 9.2 b–j. Om inget av undantagen i leden b–j är tillämpliga, är det enda lagliga undantaget för att behandla sådana uppgifter att erhålla uttryckligt samtycke i enlighet med villkoren för giltigt samtycke i GDPR.” För uttryckligt samtycke enligt artikel 9.2 a i dataskyddsförordningen krävs det att samtliga krav i nämnda förordning är uppfyllda.

5.5 Situationer när det saknas ett lämpligt undantag

58. Såsom angetts ovan är förbudet i artikel 9.1 tillämpligt om tjänsteleverantören inte kan visa att ett av undantagen föreligger. I detta fall kan tekniska åtgärder vidtas för att förhindra behandling av särskilda kategorier av personuppgifter, till exempel genom att förhindra behandling av vissa uppgifter. I detta avseende kan betaltjänstleverantörer undersöka de tekniska möjligheterna att utesluta särskilda kategorier av personuppgifter och tillåta en utvald tillgång som skulle förhindra behandling från tredjepartsleverantörer av särskilda kategorier av personuppgifter som hänför sig till passiva parter.

[33] Dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/ 679, punkt 99.

6 UPPGIFTSMINIMERING, SÄKERHET, ÖPPENHET, ANSVARSSKYLDIGHET OCH PROFILERING

6.1 Uppgiftsminimering samt inbyggt dataskydd och dataskydd som standard

59. Principen om uppgiftsminimering erkänns i artikel 5.1 c i dataskyddsförordningen, i vilken följande föreskrivs: ”Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för”. Enligt principen om uppgiftsminimering bör personuppgiftsansvariga inte behandla fler personuppgifter än vad som är nödvändigt för att uppnå det särskilda ändamålet. Såsom påpekas i kapitel 2 är det grundläggande och ömsesidigt förstådda ändamålet med avtalet avgörande för mängden och arten av personuppgifter som är nödvändiga för att tillhandahålla betaltjänsten[34]. Principen om uppgiftsminimering är tillämplig på all behandling (dvs. varje insamling av eller tillgång till och begäran om personuppgifter). I dataskyddsstyrelsens riktlinjer *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard enligt artikel 25) anges följande: ”processors and technology providers are also recognised as key enablers for DPbDD, they should also be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection[35].”

60. I artikel 25 i dataskyddsförordningen föreskrivs en skyldighet att tillämpa inbyggt dataskydd och dataskydd som standard. Dessa skyldigheter är särskilt viktiga för principen om uppgiftsminimering. I denna artikel fastställs att personuppgiftsansvariga ska, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder, vilka är utformade för ett effektivt genomförande av dataskyddsprinciper och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Dessa åtgärder kan omfatta kryptering, pseudonymisering och andra tekniska åtgärder.

61. När skyldigheten i artikel 25 i dataskyddsförordningen tillämpas ska den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter beaktas. Denna skyldighet specificeras ytterligare i dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard enligt artikel 25, till vilka hänvisats ovan.

6.2 Åtgärder för uppgiftsminimering

62. De tredjepartsleverantörer som får tillgång till betalkontouppgifter för att tillhandahålla de begärda tjänsterna måste även beakta principen om uppgiftsminimering och får endast samla in personuppgifter som är nödvändiga för att tillhandahålla de särskilda betaltjänster som betaltjänstanvändaren begärt. I princip ska tillgången till personuppgifter begränsas till vad som är nödvändigt för att tillhandahålla betaltjänster. Såsom har påpekats i kapitel 2 medför andra betaltjänstdirektivet en skyldighet för kontoförvaltande betaltjänstleverantörer att dela med sig

[34] Dataskyddsstyrelsens riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, punkt 32.
[35] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (inte översatt till svenska), sidan 29.

av betaltjänstanvändarens information på dennes begäran om betaltjänstanvändaren vill använda en betalningsinitieringstjänst eller en kontoinformationstjänst.

63. Om inte alla betalkontouppgifter är nödvändiga för att fullgöra avtalet bör leverantören av kontoinformationstjänsten välja ut de relevanta uppgiftskategorierna innan uppgifterna samlas in. Kategorier av uppgifter som inte är nödvändiga kan exempelvis omfatta den passiva partens identitet och transaktionens karaktär. Vidare behöver inte IBAN-numret från den passiva partens bankkonto anges, såvida detta inte krävs enligt medlemsstaternas nationella rätt eller EU-rätten.

64. I detta hänseende kan en eventuell tillämpning av tekniska åtgärder som möjliggör eller stödjer tredjepartsleverantörer när det gäller deras skyldighet att endast få tillgång till och hämta de personuppgifter som är nödvändiga för tillhandahållandet av deras tjänster övervägas, som del av genomförandet av lämpliga strategier för dataskydd i enlighet med artikel 24.2 i dataskyddsförordningen. För att stödja leverantörer av kontoinformationstjänster i deras skyldighet att endast samla in personuppgifter som är nödvändiga för de ändamål som de behandlas för rekommenderar styrelsen en användning av digitala verktyg. Om en tjänsteleverantör exempelvis inte behöver ha kännedom om vilken slags transaktion det är frågan om (i det beskrivande fältet i transaktionsregistret) för att tillhandahålla tjänsten kan ett digitalt urvalsverktyg fungera som ett medel för tredjepartsleverantörer för att utesluta detta fält från deras sammantagna behandling.

Exempel 2:

HappyPayments, leverantören av kontotjänster från exempel 1, vill försäkra sig om att företaget endast behandlar de personliga betalkontouppgifter som dess användare är intresserade av. Det är inte nödvändigt för tillhandahållandet av tjänsten att begära tillgång till fler betalkontouppgifter. Därför ger företaget användarna möjlighet att välja vilka särskilda typer av information de är intresserade av.

Användare A vill ha en överblick över sina utgifter under de senaste två månaderna. Således efterfrågar A information om alla transaktioner under de senaste två månaderna, transaktionsbeloppet, datumet för utförandet och mottagarens namn för sina två bankkonton hos två olika kontoförvaltande betaltjänstleverantörer och kryssar för de motsvarande rutorna i HappyPayments användargränssnitt.

HappyPayments begär sedan endast den information från de respektive kontoförvaltande betaltjänstleverantörerna som motsvarar de fält som användare A har kryssat för och endast för de senaste två månaderna. Företaget begär inte information såsom ”kommunikationen” från överföringen eller till och med IBAN, eftersom användare A inte har efterfrågat denna information.

För att HappyPayments ska kunna uppfylla sina skyldigheter vad gäller uppgiftsminimering får företaget begära tillgång till särskilda fält för en rad datum från de kontoförvaltande betaltjänstleverantörerna.

65. I detta hänseende ska det även noteras att kontoförvaltande betaltjänstleverantörer endast får ge tillgång till betaltjänstinformation enligt andra betaltjänstdirektivet. Andra betaltjänstdirektivet utgör inte någon rättslig grund för att ge tillgång till personuppgifter från andra konton, såsom sparande, lån eller investeringskonton. Således måste tekniska åtgärder vidtas enligt andra betaltjänstdirektivet för att säkerställa att tillgången är begränsad till den betalkontoinformation som är nödvändig.

66. Förutom att samla in så lite uppgifter som möjligt är tjänsteleverantören även skyldig att genomföra begränsade lagringsperioder. Tjänsteleverantören bör inte lagra personuppgifter

längre än vad som är nödvändigt i förhållande till de ändamål som betaltjänstanvändaren har efterfrågat.

67. Om avtalet mellan den registrerade och leverantören av kontoinformationstjänster kräver överföring av personuppgifter till tredje man får endast de personuppgifter som är nödvändiga för fullgörandet av avtalet överföras. Registrerade bör även erhålla särskild information om överföringen och de personuppgifter som ska överföras till denna tredje man.

6.3 Säkerhet

68. Styrelsen har redan framhållit att åsidosättandet av finansiella personuppgifter ”entydigt får allvarliga konsekvenser för den registrerades dagliga liv” och som exempel hänvisat till risken för betalningsbedrägeri[36].

69. Om en personuppgiftsincident omfatta finansiella uppgifter kan den registrerade utsättas för betydande risker. Beroende på vilken information som har läckts kan registrerade utsättas för risk för identitetskapning och att medel på deras konton och andra tillgångar stjäls. Det är även möjligt att exponeringen av transaktionsuppgifter medför betydande risker för integritetsskyddet, eftersom transaktionsuppgifter kan innehålla hänvisningar till alla möjliga aspekter av den registrerades privatliv. Samtidigt är det uppenbart att finansiella uppgifter är värdefulla för brottslingar och därför utgör ett attraktivt mål.

70. Betaltjänstleverantörer är i egenskap av personuppgiftsansvariga skyldiga att vidta lämpliga åtgärder för att skydda de registrerades personuppgifter (artikel 24.1 i dataskyddsförordningen). Ju högre risker som är kopplade till den personuppgiftsansvariges behandling, desto högre säkerhetsstandarder behöver tillämpas. Eftersom behandlingen av finansiella uppgifter medför en rad olika allvarliga risker bör säkerhetsåtgärderna således vara höga.

71. Tjänsteleverantörer bör uppfylla höga standarder, inbegripet mekanismer för stark kundautentisering och höga säkerhetsnivåer för teknisk utrustning[37]. Vidare är även andra förfaranden viktiga, såsom granskning av personuppgiftsbiträden vad gäller säkerhetsstandarder och införande av förfaranden mot obehörig tillgång.

6.4 Öppenhet och ansvar

72. Öppenhet och ansvar utgör två centrala principer i dataskyddsförordningen.

73. Vad gäller öppenhet (artikel 5.1 a i dataskyddsförordningen), föreskrivs i artikel 12 i dataskyddsförordningen att personuppgiftsansvariga ska vidta lämpliga åtgärder för att tillhandahålla all information som avses i artiklarna 13 och 14 i dataskyddsförordningen. Vidare krävs det att informationen eller kommunikationen beträffande behandlingen av personuppgifter ska vara i en koncis, klar och tydlig, begriplig och lätt tillgänglig form. Informationen ska vara i klart och tydligt språk samt skriftlig ”eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form”. Artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679 som godkänts av dataskyddsstyrelsen, erbjuder särskild vägledning om iakttagande av öppenhetsprincipen i digitala miljöer.

74. Enligt ovannämnda riktlinjer om öppenhet enligt förordning (EU) 2016/679, bör artikel 11 i dataskyddsförordningen tolkas som ett sätt att genomföra en genuin minimering av uppgifter,

[36] Artikel 29-gruppens 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, WP248 rev. 1, som godkänts av styrelsen.
[37] Se de tekniska tillsynsstandarderna.

men utan att hindra utövandet av den registrerades rättigheter och att utövandet av dessa rättigheter ska möjliggöras med hjälp av kompletterande uppgifter som tillhandahållits av den registrerade. Det kan finnas situationer där en personuppgiftsansvarig behandlar personuppgifter som inte innebär att den registrerade måste identifieras (t.ex. pseudonymiserade uppgifter). I sådana fall kan artikel 11.1 också vara relevant, eftersom det där anges att den personuppgiftsansvarige inte ska vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade enbart för att följa dataskyddsförordningen.

75. Vad gäller tjänsterna enligt andra betaltjänstdirektivet är artikel 13 i dataskyddsförordningen tillämplig på de personuppgifter som samlats in från de registrerade och artikel 14 är tillämplig när personuppgifter inte har erhållits från den registrerade.

76. I synnerhet ska den registrerade erhålla information om den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period och, i tillämpliga fall, den personuppgiftsansvariges eller en eventuell tredje parts berättigade intressen. Om behandlingen grundas på samtycke enligt artikel 6.1 a i dataskyddsförordningen eller uttryckligt samtycke enligt artikel 9.2 a i dataskyddsförordningen, krävs det att den registrerade informeras om rätten att när som helst återkalla sitt samtycke.

77. Den personuppgiftsansvarige ska lämna informationen till den registrerade med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas. Om personuppgifterna ska användas för kommunikation med den registrerade[38], vilket sannolikt är fallet i frågan om leverantörer av kontoinformationstjänster, ska informationen tillhandahållas senast vid tidpunkten för den första kommunikationen med den registrerade. Om personuppgifter ska lämnas ut till en annan mottagare ska informationen tillhandahållas senast när personuppgifterna lämnas ut för första gången.

78. När det gäller betaltjänster online klargörs det i ovannämnda riktlinjer att personuppgiftsansvariga kan tillämpa en skiktad metod där de väljer att använda en kombination av metoder för att säkerställa öppenhet. Det rekommenderas framför allt att skiktade integritetspolicyer/integritetsmeddelanden bör användas för att länka till de olika kategorier av information som måste ges till de registrerade, i stället för att visa all sådan information i ett och samma meddelande på skärmen. Syftet med detta är att undvika informationsutmattning samtidigt som det säkerställs att informationen är effektiv.

79. I ovannämnda riktlinjer klargörs även att personuppgiftsansvariga kan välja att använda ytterligare verktyg för att tillhandahålla enskilda registrerade information, såsom sekretesspaneler. Via en sekretesspanel kan de registrerade ta del av ”integritetsinformation” och ange sina integritetsrelaterade önskemål genom att tillåta eller förhindra att deras personuppgifter används på vissa sätt av den personuppgiftsansvarige i fråga[39]. En sekretesspanel kan ge en överblick över de tredjepartsleverantörer som har erhållit uttryckligt samtycke från den registrerade och kan även erbjuda relevant information om arten och mängden av personuppgifter som

[38] Artikel 14.3 b i dataskyddsförordningen.

[39] Enligt artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679 som godkänts av dataskyddsstyrelsen, är sekretesspaneler särskilt användbara när de registrerade använder samma tjänst på flera olika utrustningar, eftersom det ger dem tillgång till och kontroll över sina personuppgifter oavsett hur de använder tjänsten. Genom att ge de registrerade möjlighet att anpassa sina sekretessinställningar via en sekretesspanel kan man lättare individanpassa integritetspolicyer/integritetsmeddelanden genom att endast ange de behandlingstyper som är relevanta för den registrerade.

tredjepartsleverantörer har fått tillgång till. I princip kan en kontoförvaltande betaltjänstleverantör erbjuda användaren en möjlighet att återkalla särskilt uttryckligt samtycke enligt andra betaltjänstdirektivet[40] genom denna överblick, vilket skulle medföra nekad tillgång till deras betalkonton för en eller flera tredjepartleverantörer. Användaren kan även begära att en kontoförvaltande betaltjänstleverantör nekar tillgång till deras betalkonto(n) till en eller flera särskilda tredjepartleverantörer[41], eftersom användaren har rätt att (inte) använda en kontoinformationstjänst. Om sekretesspaneler används för att lämna eller återkalla ett uttryckligt samtycke bör de utformas och tillämpas på ett lagligt sätt och särskilt förhindra att det uppstår hinder mot tredjepartleverantörens rätt att tillhandahålla tjänster i enlighet med andra betaltjänstdirektivet. I detta hänseende och i enlighet med de tillämpliga bestämmelserna i andra betaltjänstdirektivet har en tredjepartsleverantör möjlighet att på nytt erhålla uttryckligt samtycke från användaren efter det att detta samtycke har återkallats.

80. Enligt ansvarsprincipen är den personuppgiftsansvarige skyldig att fastställa lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen, i synnerhet i överensstämmelse med de centrala principerna för dataskydd som föreskrivs i artikel 5.1. I samband med dessa åtgärder bör behandlingens art, omfattning, sammanhang och ändamål beaktas samt risken för fysiska personers rättigheter och friheter och de ska ses över och uppdateras vid behov[42].

6.5 Profilering

81. Betaltjänstleverantörernas behandling av personuppgifter kan innehålla ”profilering” enligt artikel 4.4 i dataskyddsförordningen. Till exempel kan leverantörer av kontoinformationstjänster använda sig av automatisk behandling av personuppgifter för bedömning av fysiska personers personliga aspekter. En registrerads finansiella situation kan bedömas, beroende på tjänstens specifika innehåll. Kontoinformationstjänster som ska tillhandahållas på användarnas begäran kan omfatta en omfattande bedömning av personliga betalkontouppgifter.

82. Den personuppgiftsansvarige ska även vara öppen mot den registrerade när det gäller förekomsten av automatiserat beslutsfattande, inbegripet profilering. I dessa fall ska den personuppgiftsansvarige lämna meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (artiklarna 13.2 f och 14.2 g och skäl 60)[43]. Enligt artikel 15 i dataskyddsförordningen har den registrerade rätt att begära och erhålla information från den personuppgiftsansvarige om förekomsten av automatiserat beslutsfattande, inbegripet profilering, logiken bakom samt betydelsen för den registrerade och, under vissa förutsättningar, en rätt att göra invändningar mot profilering, oberoende huruvida det enbart är frågan om automatiserat individuellt beslutsfattande som baseras på profilering[44].

83. Vidare är rätten för den registrerade att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, som föreskrivs i artikel 22 i dataskyddsförordningen relevant i detta sammanhang. Denna bestämmelse omfattar även, under

[40] Se, till exempel, det ”uttryckliga godkännande” till vilket hänvisas i artikel 67.2 a i andra betaltjänstdirektivet.
[41] Se även EBA/OP/2020/10, punkt 45.
[42] Artiklarna 5.2 och 24 i dataskyddsförordningen.
[43] Riktlinjer om öppenhet enligt förordning (EU) 2016/679, WP 260 rev.01, som godkänts av dataskyddsstyrelsen.
[44] Artikel 29-gruppen riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, WP251, rev.01.

vissa omständigheter, en skyldighet för personuppgiftsansvariga att genomföra lämpliga åtgärder för att skydda den registrerades rättigheter, såsom särskild information till den registrerade, rätten till personlig kontakt vid beslutsfattandet och att kunna utrycka sin åsikt och bestrida beslutet. Såsom även anges i skäl 71 i dataskyddsförordningen innebär detta, bland annat, att registrerade bör ha rätt att inte bli föremål för ett beslut, såsom ett automatiserat avslag på en kreditansökan online utan personlig kontakt[45].

84. Automatiserat beslutsfattande, inbegripet profilering, som inbegriper särskilda kategorier av personuppgifter är endast tillåtet om följande kumulativa villkor i artikel 22.4 i dataskyddsförordningen är uppfyllda:

- Ett undantag enligt artikel 22.2 kan tillämpas.
- Artikel 9.2 a eller g i dataskyddsförordningen är tillämplig. I båda fallen ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen[46].

85. Vidare ska även de krav på ytterligare behandling som anges i dessa riktlinjer iakttas. Förtydligandena och anvisningarna om automatiserat individuellt beslutsfattande och profilering i artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 som godkänts av dataskyddsstyrelsen är i högsta grad relevanta i samband med betaltjänster och bör därför vederbörligen beaktas.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)

[45] Skäl 71 i dataskyddsförordningen.
[46] Artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, WP251, rev.01, sidan 24.