Riktlinjer 6/2020 om samspelet mellan 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	15 december	Antagande av riktlinjerna efter sar
Version	17 juli 2020	Antagande av riktlinjerna inför off

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit f

med beaktande av artikel 70.1 e i Europaparlamentets och rådets f
april 2016 om skydd för fysiska personer med avseende på behandl
fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (

med beaktande av avtalet om Europeiska ekonomiska samarbetsområdet, särskilt bilaga XI och protokoll 37, ändrat ge
kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i sin arbetsordning,

av följande skäl:

1) Den allmänna dataskyddsförordningen tillhandahåller ett enhet
personuppgifter inom hela EU.

2) Genom andra betaltjänstdirektivet (Europaparlamentets och råde
23 december 2015 om betaltjänster i den inre marknaden, om ändring av direktiv 2007/64/EG. Vidare
bestämmelser för att säkerställa rättssäkerhet för konsumenter,
betalningskedjan samt moderniseras och underlättas regelverket för betaltjän[2].
Medlemsländerna skulle ha införlivat andra betaltjänstdirektivet i
den 13 januari 2018.

3) En viktig del av andra betaltjänstdirektivet utgör inte framför det av
betalningsinitiering och kontoinformationstjänster. Direktivet gö
betaltjänstleverantörer att erhålla tillgång till registrerades betal
nämnda tjänster.

4) Vad gäller dataskydd bör behandling av personuppgifter enligt artike
betaltjänstdirektivet, inbegripet tillhandahållande av information
direktiv utföras i enlighet med dataskyddsförordningen (EU) 2018/1725[3].

5) I skäl 89 i betaltjänstdirektivet anges att när personuppgifter b
direktivet bör det exakta syftet anges, tillämplig rättslig grund å
dataskyddsförordningen följas och principerna om minimering av uppgifter,
ändamålsbegränsning och proportionerlig lagringstid för uppgifter
uppgiftsskydd och dataskydd som standard ingå i alla databehan
används inom ramen för andra betaltjänstdirektivet[4].

6) I skäl 93 i andra betaltjänstdirektivet anges att leverantörerna
leverantörerna av kontoinformationstjänster, å ena sidan, o
betaltjänstleverantören, å andra sidan, bör vidta lämpliga säkerhetsåtgärder som
fastställs eller som avses i detta direktiv eller som ingår i teknisk

[1] Hänvisningar till medlemsstater i detta dokument bör förstås som hänvi
[2] Skäl 6 i andra betaltjänstdirektivet.
[3] Eftersom andra betaltjänstdirektivet antogs före dataskyddsförordningen
95/46. I artikel 94 i dataskyddsförordningen föreskrivs att hänvisningar ti
anses som hänvisningar till den förordningen.
[4] Skäl 89 i andra betaltjänstdirektivet.

HÄRIGENOM FÖRESKRIVS.

1. INLEDNING

1. Genom andra betaltjänstdirektivet har ett antal nyheter införts. Medan detta skapar nya möjligheter för konsumenter och ökar ins tillämpningen av andra betaltjänstdirektivet att det uppkommer gäller kravet på att registrerade ska behålla full kontroll över Den al dataskyddsförordningen (dataskyddsförordningen) är tillämplig på behandling av perso inbegripet behandling som genomförs i samband med betaltjänst betaltjänstdirektivet.[5] Således ska personuppgiftsansvariga som är verksamma som omfattas av andra betaltjänstdirektivet alltid säkerställa personuppgifter som föreskrivs i artikel 5 i dataskyddsförordningen bestämmelserna i direktivet om integritet och elektronisk kommunikation.[6] Samtidigt innehåller andra betaltjänstdirektivet[7] och de tekniska tillsynsstandarderna för sträng gemensamma och säkra öppna kommunikationsstandarder (de tekniska tillsynsstandarderna)[8] innehåller vissa bestämmelser om dataskydd och datasäkerhet beträffande tolkningen av dessa bestämmelser samt samspelet dataskydd och andra betaltjänstdirektivet.

2. Den 5 juli 2018 antog dataskyddsstyrelsen en skrivelse om andra betalt styrelsen klargjorde frågor som rörde skydd av personuppgif betaltjänstdirektivet, särskilt behandling av personuppgifter från avtalsslutande parter (uppgifter från passiva parter) från leverantörer av kontoinforma betalningsinitieringstjänster, förfarandena för att lämna och å tillsynsstandarderna och samarbete mellan betaltjänstleverantörer som förvaltar konto gäller säkerhetsåtgärder. Det förberedande arbetet med dessa r synpunkter från berörda parter, både skriftligt och vid en samma att identifiera de mest brådskande utmaningarna.

3. Syftet med dessa riktlinjer är att tillhandahålla ytterligare väg samband med andra betaltjänstdirektivet, i synnerhet om förh bestämmelserna i dataskyddsförordningen och andra betaltjänstdirektivet. Tyngdpunkten riktlinjer ligger på behandlingen av personuppgifter f kontoinformationstjänster och betalningsinitieringstjänster. I de för att bevilja tillgång till betalkonton från kontoförvaltande betaltjänstle för behandling av personuppgifter från leverantörer av beta

---

[5] Artikel 1.1 i dataskyddsförordningen.

[6] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 o och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektr 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 Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstanda kundautentisering och gemensamma och säkra öppna kommunikationsstand 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:32018R0389&from=SV

kontoinformationstjänster, inbegripet villkor och skyddsåtgärde personuppgifter från leverantörer av betalningsinitieringstjänster och för andra ändamål än de för vilka de ursprungligen samlades in, in inom ramen för tillhandahållandet av[9]. En kontoinformationstjä även olika begrepp i samband med uttryckligt samtycke enligt dataskyddsförordningen, behandling av uppgifter från passiva kategorier av personuppgifter från leverantörer av betalningsinitierin kontoinformationstjänster, tillämpning av de centrala principern dataskyddsförordningen, inbegripet uppgiftsminimering, öppenhe Andra betalskyddsdirektivet är funktionellt ansvar inom bland an konsumentskydd och konkurrensrätt. Dessa riktlinjer omfattar in rättsområden.

4. För att underlätta läsningen av dessa riktlinjer tillhandahålls de i detta dokument nedan.

1.1 Definitioner

Leverantör av kontoinformationstjänst: leverantör av en onlinetjänst för att sammanställd information om ett eller flera betalkonton som beta antingen annan betaltjänstleverantör eller hos fler än en betaltjänstl

Kontoförvaltande betaltjänstleverantör: betaltjänstleverantör som tillhandahålle betalkonto för en betalare.

Uppgiftsminimering: dataskyddsprincip enligt vilken personuppgifter ska vara adekvata och inte för omfattande i förhållande till de ändamål för vilka de b

Betalare: en fysisk eller juridisk person som är betalkontoinnehava betalningsorder från detta betalkonto, eller om det inte finns något betalkonto av detta, en fysisk eller ju lämnar en betalningsorder.

Betalningsmottagare: en fysisk eller juridisk person som är den avsedda mo omfattats av en betalningstransaktion.

Betalkonto: ett konto i en eller flera betaltjänstanvändares namn för användni av betalningstransaktioner.

Leverantör av betalningsinitieringstjänster: leverantör av en tjänst för att initiera e på begäran av betaltjänstanvändaren med ett betalkonto som innehas hos en an betaltjänstleverantör.

Betaltjänstleverantör: ett organ som avses i artikel 1.1 i[10] andra betaltjänst eller juridisk person som omfattas av ett undantag enligt artiklarna

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

[10] I artikel 1.1 i andra betaltjänstdirektivet fastställs hur medlemsstaterna ska skilja mellan följande kategorier av betaltjänstleverantörer:

a) Kreditinstitut enligt definitionen i artikel 4.1.1 i Europaparlamentets o 575/2013, inbegripet filialer till dessa enligt definitionen i artikel 4.1.17 i den förordningen, när dessa

Betaltjänstanvändare: en fysisk eller en juridisk person som utnyttjar en betalare, betalningsmottagare eller båda.

Personuppgifter: varje upplysning som avser en identifierad eller ident registrerad). En identifierbar fysisk person är en person som direkt el synnerhet genom hänvisning till en identifierare som ett namn, ett identifikationsnum lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera fysiska personens fysiska, fysiologiska, genetiska, psykiska, ek identitet.

Inbyggt dataskydd: tekniska och organisatoriska åtgärder som ingår i en utformade för ett effektivt genomförande av dataskyddsprinciper oc skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls o registrerades rättigheter skyddas.

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

Tekniska tillsynsstandarder: kommissionens delegerade förordning (EU) 2018/3 2017 om komplettering av Europaparlamentets och rådets direktiv (tillsynsstandarder för sträng kundautentisering och gemensa kommunikationsstandarder.

Tredjepartsleverantörer: både leverantörer av betalningsinitieringstjänster o kontoinformationstjänster.

1.2 Tjänster enligt andra betaltjänstdirektivet

5. I andra betaltjänstdirektivet införs två nya typer av betaltjäns betalningsinitieringstjänster och kontoinformationstjänster. betaltjänstdirektivet innehåller åtta betaltjänster som omfattas

6. Leverantörer av betalningsinitieringstjänster tillhandahåller betalningsorder på betaltjänstanvändarens begäran med avsee användaren innehar hos en annan betaltjänstleverantör[11]. En leverantör av betalningsinitieringstjänster kan begära att en kontoförvaltande

inom unionen, antingen huvudkontoret för de filialerna är belägna inom un i direktiv 2013/36/EU och med nationell rätt, utanför unionen.
b) Institut för elektroniska pengar enligt definitionen i artikel 2.1 i direktiv 2 med artikel 8 i det direktivet och med nationell rätt, filialer till dessa när och deras huvudkontor är beläget utanför unionen, i den mån de betaltjänster som tillh filialer är knutna till utgivning av elektroniska pengar.
c) Postgiroinstitut som enligt nationell rätt har rätt att tillhandahålla bet
d) Betalningsinstitut.
e) ECB och nationella centralbanker, när de inte agerar i egenskap av monetär myndigheter.
f) Medlemsstaterna eller deras regionala eller lokala myndigheter, när de myndigheter.

[11] Artikel 4.15 i andra betaltjänstdirektivet.

bank) initierar en transaktion för betaltjänstanvändarens räkni vara en fysisk person (registrerad) eller en juridisk person.

7. Leverantörer av kontoinformationstjänster tillhandahåller onli information om ett eller flera betalkonton som betaltjänstanvän annan betaltjänstleverantör eller flera betaltjänstleverantörer.[12] Enligt skäl 28 i and betaltjänstdirektivet ska betaltjänstanvändaren ha möjlighet att få överblick över sin ekonomiska situation.

8. I fråga om kontoinformationstjänster kan flera olika typer av tjänster erbjudas, med utgångspunkt i olika särdrag och syften. Vissa leverantörer kan till exempel er budgetplanering och övervakning av utgifter. Andra betaltjän behandling av personuppgifter i dessa tjänster. Direktivet är inte tjänster som omfattar kreditbedömningar av betaltjänstanvändar genomförs på grundval av en insamling av information via en ko tjänster omfattas därför av dataskyddsförordningen. Vidare är andra heller tillämpligt på andra konton än betalkonton (t.ex. sp Dataskyddsförordningen utgör under alla omständigheter den t behandlingen av personuppgifter.

Exempel 1: HappyPayments är ett företag som erbjuder en onlinetjä information om ett eller flera betalkonton genom en mob överblick (en kontoinformationstjänst). Med denna tjänst kan be över saldon och nyligen genomförda transaktioner i två e betaltjänstanvändaren väljer det, erbjuder företaget en tjänst för att dela in utgi inkomster i olika kategorier (lön, fritid, energi, bolån osv med dennes ekonomiska planering. I denna app erbjuder initiera betalningar direkt från de anknutna betalni betalningsinitieringstjänst).

9. För att dessa tjänster ska kunna tillhandahållas regleras de rätt betalningsinitieringstjänster och kontoinformationstjänster. Betaltjänstleverantörer kan f tillhandahålla en tjänst till betaltjänstanvändaren i andra betalt

10. I artiklarna 66.1 och 67.1 i andra betaltjänstdirektivet föreskrivs till tillgång till och användning av betalningsinitierings- och kontoinformationstjänster. Detta in bör stå betaltjänstanvändaren helt fritt att utöva en sådan rättig att använda denna rättighet.

11. Tillgång till betalkonton och användning av kontoinformation regleras av artiklarna 66 och 67 i andra betaltjänstdirektivet, vilket innehåller skyd (person)uppgifter. I artikel 66.3 f i andra betaltjänstdirektiv betalningsinitieringstjänster inte får begära av betaltjänstanvändaren andra uppgifter än dem som krävs för att tillhandahålla betalningsinitieringstjänsten o föreskrivs att leverantörer av betalningsinitieringstjänster inte lagra uppgifter för andra ändamål än för att tillhandahålla den betal uttryckligen begärs av betaltjänstanvändaren. Enligt artikel 67.2

[12] Artikel 4.16 i andra betaltjänstdirektivet.

vidare leverantörer av kontoinformationstjänster information från t
betecknade betalkonton och dithörande betalningstransaktionen
direktivet föreskrivs att leverantörer av kontoinformationstjänste
eller lagra några uppgifter från för andra ändamål än för att genomföra
kontoinformationstjänst som betaltjänstanvändaren uttryckligen
uppgiftsskyddsreglerna om uppgiftsskydd. I dessa regler framhål
samlas in för särskilda, uttryckligt berättigade ändamål inom
kontoinformationstjänster. En leverantör av kontoinformationstj
ange i avtalet för vilka särskilda ändamål personliga kontoinfo
behandlas i samband med kontoinformationstjänster denne tillhandahå
dataskyddsförordningen ska avtalet vara lagligt, korrekt och öp
konsumentlagstiftning.

12. Beroende på särskilda omständigheter kan utöver betaltjäns
personuppgiftsansvariga eller personuppgiftsbiträden enligt da
riktlinjer är de betaltjänstleverantörer som, själva eller tillsa
ändamålen med och medlen för behandling av personuppgifter som
vägledning om detta finns i dataskyddsstyrelsens riktlinjer
personuppgiftsansvarig och personuppgiftsbiträde enligt datasky

2 LAGLIGA GRUNDER OCH VIDARE BEHANDLING ENLIGT ANDRA BETALTJÄNSTDIREKTIVET

2.1 Lagliga grunder för behandling

13. Enligt dataskyddsförordningen ska personuppgiftsansvariga ha e personuppgifter. Artikel 6.1 i dataskyddsförordningen inneh begränsande förteckning över sex rättsliga grunder för behandling av person dataskyddsförordningen.[13] Det ankommer på den personuppgiftsansvarige lämpliga rättsliga grunden och säkerställa att samtliga villko fastställa vilken grund som är giltig och mest lämplig i en sä omständigheter under vilka behandlingen äger rum, inbegripet än förhållandet mellan den personuppgiftsansvarige och den registr

2.2 Artikel 6.1 b i dataskyddsförordningen (behandlingen är nödvä fullgöra ett avtal)

14. Betalningstjänster tillhandahålls på grund av ett avtal mella betaltjänstleverantören. I skäl 87 i andra betaltjänstdirektivet a gälla skyldigheter och ansvar enligt avtalet mellan betaltjä betaltjänstleverantör. När det gäller dataskyddsförordningen u grunden för behandling av personuppgifter i samband med tillhandahållande b i dataskyddsförordningen, vilket innebär att behandlingen är n i vilket den registrerade är part eller för att vidta åtgärder på b ett sådant avtal ingås.

15. Betalningstjänsterna enligt andra betaltjänstdirektivet definiera Tillhandahållandet av dessa tjänster såsom de definieras enligt ett villkor för att det ska uppkomma ett avtal mellan parterna är tillgång betaltjänstanvändarens betalkontouppgifter. Dessa betaltjänst auktoriserade aktörer. I förhållande till betalningsin kontoinformationstjänster enligt andra betaltjänstdirektivet kan villk

---

[13] Enligt artikel 6 är behandlingen endast laglig om och i den mån som åtm uppfyllda:

(a) Den registrerade har lämnat sitt samtycke till att hans eller hennes personuppgifter behandlas för ett el specifika ändamål.

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

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

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

(e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller s personuppgiftsansvariges myndighetsutövning.

(f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsa berättigade intressen, om inte den registrerades intressen eller grundläggande rättigh väger tyngre och kräver skydd av personuppgifter, särskilt när den r

ytterligare tjänster som inte är reglerade i andra betaltjänstdi riktlinjer 2/2019 om behandling av personuppgifter enligt artikel samband med tillhandahållandet av onlinetjänster till registrerade, personuppgiftsansvariga ska bedöma vilken behandling av perso nödvändig för fullgörandet av avtalet. I dessa riktlinjer påpekas är nödvändig beror på vad för slags tjänst det är frågan om, avtalsp och förväntningar, avtalets logiska grund och avtalets grundsats

16. I dataskyddsstyrelsens riktlinjer 2/2019 klargörs även att det, dataskyddsförordningen, görs skillnad mellan behandling som är avtal och klausuler som gör tjänsten beroende av viss behandlin inte är nödvändig för avtalets fullgörande. Nödvändighet för fullg utöver ett avtal.[14] Den personuppgiftsansvarige bör kunna visa hur angivna avtalet med den registrerade rent faktiskt inte kan behandlingen av personuppgifterna i fråga. Att endast hänvisa till uppgiftsbehandling i ett avtal räcker inte för att behandlingen i 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, uttr ändamål och inte senare behandlas på ett sätt som är oförenlig bedömer om artikel 6.1 b är en lämplig rättslig grund för behandling i samband med en online, bör man ta hänsyn till tjänstens särskilda ändamål, syfte eller e[15] Ändamålen med behandlingen måste anges tydligt och meddelas till den regis personuppgiftsansvariges ändamålsbegränsnings- och öppenhetsskyldigheter. Att bed som är nödvändigt innebär en kombinerad, faktabaserad bedöm mål som åsyftas och av huruvida det är mindre integritetskränka för hur man uppnår samma mål. Artikel 6.1 b omfattar inte behand objektivt sett inte nödvändig för att utföra den avtalade tjänste avtalsförberedande åtgärderna på den registrerades begäran, även om de är nödvändiga för den personuppgiftsansvariges andra verksamhetsändamål.[16]

18. I dataskyddsstyrelsens riktlinjer 2/2019 klargörs att ett avtal kategorierna av personuppgifter eller de typer av behandling som angivna måste utföra för fullgörandet av avtalet i den mening som avses i riktlinjerna.[17] behandlas även fall i vilka ett antal situationer kan uppkomma för registrerad endast är intresserade av en av tjänsterna. Detta kan personuppgiftsans skapa ett paket av flera fristående tjänster eller delar av en ändamål, kännetecken eller motivering i ett enda avtal. Om ett tjänster eller delar av en tjänst som i själva verket rimligen kan utföras ob tillämpningen av artikel 6.1 b bedömas mot bakgrund av var oc genom att man tittar på vad som objektivt sett är nödvändigt f enskilda tjänster som den registrerade aktivt har begärt eller an[18]

---

[14] Dataskyddsstyrelsens riktlinjer 2/2019 om behandling av personuppgifter dataskyddsförordningen i samband med tillhandahållandet av onlinetjänste

[15] Ibid.

[16] Ibid, sidan 7.

[17] Ibid, sidan 10.

[18] Ibid, sidan 11.

19. I överensstämmelse med ovannämnda riktlinjer har personuppg bedöma vad som objektivt sett är nödvändigt för fullgör personuppgiftsansvariga inte kan visa att behandlingen av de p inte objektivt sett är nödvändig för tillhandahållandet av var och artikel 6.1 b i dataskyddsförordningen grund för behandlingen. I situationer bör den personuppgiftsansvarige överväga en annan

2.3 Förebyggande av bedrägerier

20. I artikel 94.1 i andra betaltjänstdirektivet föreskrivs att me betalningssystem och betaltjänstleverantörer behandlar personupp att säkerställa förebyggande, undersökning och avslöjande av behandling av personuppgifter som är absolut nödvändig för att ge ett berättigat intresse för den berörda betaltjänstleverantören registrerades intressen eller grundläggande rättigheter och f betaltjänstleverantören[19]. Behandlingen för att förhindra bedrägerier skulle grundas på en noggrann bedömning från den personuppgiftsansv med ansvarsprincipen. För att förhindra bedrägerier kan person av särskilda kategorier av personuppgifter som gör att en behandling av personupp

2.4 Ytterligare behandling (leverantörer av kontoinforma betalningsinitieringstjänster)

21. I artikel 6.4 i dataskyddsförordningen fastställs villkoren för b andra ändamål än det ändamål för vilket personuppgifterna sam ytterligare behandling genomföras som grundar sig på unionsr nationella rätt som utgör en nödvändig och proportionell åtgärd i att säkerställa de mål som avses i artikel 23.1, där den registre om en behandling för andra ändamål än det ändamål för vilket p förenlig med de regler som gäller för det ursprungliga ändamålet.

22. Artiklarna 66.3 g och 67.2 f i andra betaltjänstdirektivet måste anges det i artikel 66.3 g i andra betaltjänstdirektivet betalningsinitieringstjänster inte får använda, lagra eller få tillgång till för andra ändamål än för att tillhandahålla den betalningsinitieringstjänst som utt artikel 67.2 f i andra betaltjänstdirektivet anges att leverantörer får använda, få tillgång till eller lagra några uppgifter för några a genomföra den kontoinformationstjänst som betaltjänstanvända enlighet med uppgiftsskyddsreglerna om uppgiftsskydd.

23. Genom artiklarna 66.3 g och 67.2 f i andra betaltjänstdirektivet begrän möjligheterna till behandling för andra ändamål avsevärt, vilke ändamål endast är tillåten om den registrerade har lämnat sa dataskyddsförordningen eller behandlingen föreskrivs i unionsrätten nationella rätt som den personuppgiftsansvarige omfattas dataskyddsförordningen. Om behandlingen för andra ändamål personuppgifterna samlades inte grundas på den registrerades samtyc medlemsstaternas nationella rätt, framgår det av de begränsning g och 67.2 f i andra betaltjänstdirektivet att med det andra ändamålet inte fö

[19] Skäl 47 i dataskyddsförordningen.

vilket personuppgifterna ursprungligen samlades in. Den förenli
artikel 6.4 i dataskyddsförordningen kan inte utgöra rättslig gru

24. Enligt artikel 6.4 i dataskyddsförordningen ytterligare behandling som grund unionsrätten eller medlemsstaternas nationella rätt. Exempelv betalningsinitieringstjänster och kontoinformationstjänster ansv Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 201 förhindra att det finansiella systemet används för penningtvätt (penningtvättsdirektivet). Dessa ansvariga enheter är därför sky kundkännedom som anges i detta direktiv. De personuppgifter so tjänst enligt andra betaltjänstdirektivet behandlas därför ytter rättslig förpliktelse som åligger tjänsteleverantören[20]

25. Såsom anges i punkt 20 framgår det av artikel 6.4 i dataskyddsfö andra ändamål än det ändamål för vilket personuppgifterna sa registrerades samtycke, om samtliga villkor för samtycke i enli uppfyllda. Såsom anges ovan måste den personuppgiftsansvarig problem vägra eller ta tillbaka sitt samtycke (skäl 42 i dataskyd

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

26. Såsom anges i punkt 10 kan betaltjänstanvändare utöva sin rätt och kontoinformationstjänster. De skyldigheter som medlemsstat 67.1 i andra betaltjänstdirektivet bör införlivas i nationell rätt för att tillämpning av betaltjänstanvändarens rätt att dra nytta av ova kontoförvaltande betaltjänstleverantören, normalt sett en bank skyldighet att bevilja betaltjänstleverantören tillgång till konto uppfyller alla krav för att erhålla tillgång till betaltjänstanvä tillämpning av sådana rättigheter inte möjlig. Det anges tydligt i artiklarna 66.5 o andra betaltjänstdirektivet att tillhandahållandet av betalr kontoinformationstjänster inte får vara avhängigt av förekomsten leverantören av betalningsinitieringstjänster eller kontoinformationstjän kontoförvaltande betaltjänstleverantören.

27. Den kontoförvaltande betaltjänstleverantörens behandling av pe att bevilja tillgång till de personuppgifter som betalningsinitieringstjänst kontoinformationstjänster begär för att fullgöra sin betaltjänst ti på en rättslig förpliktelse. För att uppnå målen i andra kontoförvaltande betaltjänstleverantören tillhandahålla personuppgifterna fö leverantörerna av betalningsinitieringstjänster och kontoinform nödvändig förutsättning för att dessa ska kunna tillhandahålla garantera de rättigheter som föreskrivs i artiklarna 66.1 och 67.1 i tillämpliga rättsliga grunden i sådana fall är därför artikel 6.1 c

28. Eftersom det anges i dataskyddsförordningen att en behandling som baseras på rättslig förpliktelse tydligt ska fastställas i enlighet med unionsrätten el (se artikel 6.3 i dataskyddsförordningen), ska skyldighet

[20] Notera att detta dokument inte omfattar någon grundlig undersökning av penningtvättsdirektivet uppfyller kraven i artikel 6.4 i dataskyddsförordni

betaltjänstleverantörer att abvevdlejra ntialtigoåmeglfaölljaag stiftning genom betaltjänstdirektivet har införlivats.

3 UTTRYCKLIGT SAMTYCKE

3.1 Samtycke enligt dataskyddsförordningen

29. Enligt dataskyddsförordningen utgör samtycke en av de sex r
behandling av personuppgifter. Enligt artikel 4.11 i dataskyddsförordn
som varje slag av frivillig, specifik, informerad och otvetydig
registrerade, antingen genom ett uttalande eller genom en tydlig
behandling av personuppgifter som rör honom eller henne. För
det avgörande att dessa fyra villkor är uppfyllda, nämligen att
informerat och otvetydigt. Enligt Europeiska dataskyddsstyrelsens riktlinjer 05/2020 om sam
förordning (EU) 2016/679 kan samtycke enbart vara den lämpl
registrerade erbjuds kontroll och får en genuin valmöjlighet att
som ges eller inte kan godta dem utan problem. När den personuppg
samtycke måste han eller hon bedöma huruvida samtliga villk
erhållandet av giltigt samtycke. Om samtycke erhålls helt
dataskyddsförordningen är samtycke ett verktyg som ger de registrerad
deras personuppgifter kommer att behandlas. I annat fall blir de
samtycke kommer då att vara en ogiltig rättslig grund för behandlingen.[21]

30. Dataskyddsförordningen innehåller även ytterligare skyddsåtgär
att den personuppgiftsansvarige ska kunna visa att det förelåg g
behandlingen. Begäran om samtycke ska även läggas fram på ett sätt som
särskiljas från de andra frågorna i en begriplig och lätt tillgäng
och tydligt språk. Vidare ska den registrerade informeras om rä
samtycket lika enkelt som att lämna samtycke.

31. Enligt artikel 9 i dataskyddsförordningen utgör samtycke ett av
förbudet att behandla särskilda kategorier av personuppgifter.
emellertid att den registrerade uttryckligen lämnat samtycke.[22]

32. Enligt dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enlig
med uttryckligt samtycke enligt dataskyddsförordningen hur d
samtycke. Det innebär att den registrerade måste avge en uttrycklig
behandling för särskilda ändamål. Ett självklart sätt att se till
uttryckligen bekräfta sitt samtycke i en skriftlig förklaring. I
personuppgiftsansvarige kunna säkerställa att den skriftliga fö
registrerade, för att undanröja alla eventuella tvivel och risker

33. Under inga omständigheter kan samtycke erhållas genom tvetydiga förkl
handlingar. En personuppgiftsansvarig måste också vara medv
erhållas genom att den registrerade godtar ett avtal eller allmän

3.2 Samtycke enligt e-integritetsdirektivet

[21] Dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (
[22] Se även yttrande 15/2011 om definitionen av begreppet samtycke (WP
6/2014 om begreppet den registeransvariges berättigade intressen i artik
10, 13 och 14.

34. Styrelsen noterar att den rättsliga ramen för uttryckligt samtycke betaltjänstdirektivet och dataskyddsförordningen innehåller beg Detta leder fram till frågan huruvida såsom anges i artikel 94.2 i betaltjänstdirektivet bör tolkas på samma sätt som uttry dataskyddsförordningen.

3.2.1 Uttryckligt medgivande enligt artikel 94.2 i andra betaltj

35. Andra betaltjänstdirektivet innehåller flera bestämmelser som rör b personuppgifter, särskilt artikel 94.1 i direktivet, där det personuppgifter enligt andra betaltjänstdirektivet måste följa EU föreskriva artikel 94.2 i andra betaltjänstdirektivet att betaltjänst tillgång till, behandla och bevara sådana personuppgifter som är av betaltjänsterna, med uttryckligt medgivande. Enligt artikel 33.2 andra betaltjänstdirektivet är detta krav på uttryckligt medgiva inte tillämpligt på leverantörer av kontoinformationstjänster. E godkännande för leverantörer av kontoinformationstjänster för tillhandahållande enligt artikel 67.2 a i andra betaltjänstdirektivet.

36. Såsom angetts ovan är förteckningen över grunder för laglig beh uttömmande. Såsom anges i punkt 146 i riktlinjerna ska artikel 6.1 b i dataskyddsförordnin rättsliga grunden för behandling av personuppgifter för tillhand innebär att behandlingen är nödvändig för att fullgöra ett avtal eller för att vidta åtgärder på begäran av den registrerade innan ett så följer att artikel 94.2 i andra betaltjänstdirektivet inte kan bet grund för behandling av personuppgifter. Mot denna bakgrund bestämmelse dels ska tolkas i enlighet med den tillämpliga rätts på ett sådant sätt att dess ändamålsenliga verkan bibehålls. Utt 94.2 i andra betaltjänstdirektivet ska därför tolkas som att det[23] förhållande till tillgång till och efterföljande behandling och la tillhandahålla betaltjänster och har därför inte samma innebörd dataskyddsförordningen.

37. Uttryckligt medgivande till vilket hänvisas i artikel 94.2 i and samtycke genom avtal. Detta innebär att artikel 94.2 i andra bet registrerade när del i ingående av ett avtal med en betaltjänstleverantör enligt andra b måste få full kännedom om vilka särskilda kategorier av pers behandlas. Vidare ska de få kännedom om det särskilda ändamål personuppgifter kommer att behandlas och uttryckligen godkänn klausuler bör klart och tydligt kunna särskiljas från de andra frå krävs att den registrerade uttryckligen godtar dem.

38. Erhållande av tillgång till personuppgifter för efterföljande behandlin uppgifter i syfte att tillhandahålla betaltjänster har central bet medgivande enligt artikel 94.2 i andra betaltjänstdirekti betaltjänstleverantörer[24] som inte behandlar personuppgifterna, utan be personuppgifter som har behandlats under ansvar av någon anna betaltjänstanvändare ingår ett avtal med, till exempel,

[23] Dataskyddsstyrelsens skrivelse om andra betaltjänstdirektivet, 5 juli 2018, si
[24] Detta är tillämpligt på tjänsterna i punkt 1 i bilagan till andra betaltjänstdirektivet.

betalningsinitieringstjänst, behöver denna leverantör erhålla t betaltjänstanvändaren som behandlas under den kontoförvalta ansvar. Syftet med det uttryckliga medgivandet enligt artikel 94.2 i andra betaltjänstdirektivet är att erhålla tillgång till dessa personuppgifter för att kunna beha som är nödvändiga för att kunna tillhandahålla betaltjänsten. uttryckligt medgivande för att kontoförvaltande betaltjänstleverantören skyldig de angivna personuppgifterna.

39. Även om medgivandet enligt artikel 94.2 i andra betaltjänstdirektivet för behandling av personuppgifter, handlar särskilt om tillgång till personuppgif dataskydd och garanterar öppenhet och en viss kontroll[25]. Med hänsyn till bet materiella villkoren för medgivande enligt artikel 94.2 i andra direktivet, bör det, när så anges, tolkas i överensstämmelse med den ramen för dataskydd samt så att dess ändamålsenliga verkan bib

40. Vad gäller den information som personuppgiftsansvariga ska tillh anges i artikel 29-gruppens riktlinjer om öppenhet [e]n viktig aspekt av beskrivs i dessa bestämmelser är att de registrerade på förhand konsekvenserna av behandlingen och att det inte bör komma som en sor senare skede hur deras personuppgifter har använts[26].

41. Personuppgifter ska vidare, i enlighet med principen om ändar särskilda, uttryckligt angivna och berättigade ändamål (artikel 5 personuppgifter samlas in för ett bestämt ändamål bör personuppgiftsansvariga undvika identifiera ett brett ändamål för att motivera olika former av ytterligare behand verket enbart har ett avlägset samband med det ursprungliga ändamålet[27]. Exempelvis i samband med avtal för nättjänster har styrelsen framhållit ris behandlingsvillkor i avtal och har angett att syftet med insam specifikt. Det måste vara tillräckligt detaljerat för att fastställa vilken typ av inbegrips och inte inbegrips i det angivna syftet, och möjliggör bedömas och uppgiftsskyddsgarantierna kan tillämpas[28].

42. Mot bakgrund av det ytterligare kravet på uttryckligt medgivande enligt artikel betaltjänstdirektivet, innebär detta att personuppgiftsansvariga och specifik information om de särskilda ändamål som den identifierat, för vilka personuppgifter hämtas, behandlas och lagr med artikel 94.2 i andra betaltjänstdirektivet måste registrerade ändamål.

43. Såsom anges ovan i punkt 10 framhåller styrelsen att betaltjänstanvändaren måste kunna välja om denne vill använda tjänsten eller inte och kan i måste medgivandet enligt artikel 94.2 i andra betaltjänstdirektiv

3.3 Slutsats

[25] Artikel 94.2 i andra betaltjänstdirektivet omfattas av kapitel 4 dataskyd

[26] Artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679, p 2018) som godkänts av dataskyddsstyrelsen.

[27] Artikel 29-gruppens yttrande 03/2013 om ändamålsbegränsning (WP203), sida

[28] Riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i med tillhandahållandet av onlinetjänster till registrerade, punkt 16 (versi 29-gruppens yttrande 03/2013 om ändamålsbegränsning (WP203), sidorna 15–16.

44. Uttryckligt medgivande enligt tjänstedirektivet skiljer sig från (uttryckl
enligt dataskyddsförordningen. Uttryckligt medgivande enlig
betaltjänstdirektivet utgör ett ytterligare krav av avtalsrä
betaltjänstleverantörer att få tillgång till och behandla personuppgifter för tillhandahållande
krävs det uttryckligt medgivande från betaltjänstanvändaren i e
betaltjänstdirektivet.

4 BEHANDLING AV UPPGIFTER FRÅN PASSIVA PAR

4.1 Uppgifter från passiva parter

45. En fråga som rör uppgiftsskydd som måste övervägas noga är b kallade passiva parter. Inom ramen för detta dokument utgör personuppgifter från en registrerad som inte är användare av en särskil personuppgifter behandlas av denna särskilda betaltjänstleveran leverantören och betaltjänstanvändaren. Detta är exempelvis fal registrerad A, använder tjänster från en leverantör av kontotjänster och regi antal betalningstransaktioner till A:s betalkonto. I denna situat parten och de personuppgifter (såsom B:s kontonummer och det omfattade) som rör B betraktas som uppgifter från passiva part

4.2 Den personuppgiftsansvariges berättigade intresse

46. Enligt artikel 5.1 b i dataskyddsförordningen krävs det att pers särskilda, uttryckligt angivna och berättigade ändamål och inte senare behand är oförenligt med dessa ändamål. I dataskyddsförordningen u behandling av personuppgifter måste vara både nödvändig överensstämma med principerna för dataskydd, såsom principerna om änd uppgiftsminimering.

47. Behandling av uppgifter från passiva parter kan vara tillåten e behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje p parts berättigade intressen (artikel 6.1 f i dataskyddsförordninge endast tillåten såvida inte den registrerades intressen eller gru väger tyngre än den personuppgiftsansvariges berättigade intressen och k personuppgifter.

48. I samband med tillhandahållande av betaltjänster enligt andra be grund för behandling av uppgifter från passiva parter betalningsinitieringstjänster och kontoinformationstjänster s personuppgiftsansvariges eller en tredje parts berättigade intr betaltjänstanvändaren. Behovet av att behandla personuppgifte begränsat till och bestäms av dessa registrerades i samband med fö tillhandahållandet av betaltjänster som omfattas av andra betal lämpliga åtgärder fastställas för att säkerställa att passiva par rättigheter och friheter och att de registrerades rimliga förvän behandlingen av deras personuppgifter respekteras. I detta h personuppgiftsansvarige (en leverantör av kontoinform betalningsinitieringstjänster) ska vidta åtgärder som är nödvändiga för skydda de registrerades intressen. Detta omfattar tekniska åtgär från passiva parter inte behandlas för andra ändamål än det änd betalningsinitieringstjänster och kontoinformationstjänster u personuppgifterna. Om det är möjligt ska även kryptering eller åstadkomma en lämplig nivå vad gäller säkerhet och uppgiftsmin

4.3 Ytterligare behandling av personuppgifter från den p

49. Såsom anges i punkt 29 kan personuppgifter som behandlas i sa som regleras i andra betaltjänstdirektivet behandlas ytterlig

förpliktelser som åvilar tjänsteleverantören. Dessa rättsliga förpli… från den passiva parten.

50. Vad gäller ytterligare behandling av uppgifter från passiva pa… intressen, anser styrelsen att uppgifterna inte kan användas för ett annat än… vilket personuppgifterna samlades in, förutom på grundval av EU-rätten eller medlemsstaternas nationella rätt. I rättsligt hänseende är det inte möjligt att inh… parten, eftersom dennes personuppgifter behöver samlas in elle… samtycke, för vilket det inte finns någon rättslig grund enligt a… Inte heller kan den förenlighetsbedömning som föreskrivs i artikel… utgöra en grund för behandling för andra ändamål (t.ex. direktma… passiva parters rättigheter och friheter respekteras inte om … använder personuppgifterna för andra ändamål, med beaktande av det sammanhang… personuppgifterna har samlats in, särskilt eftersom det inte f… registrerade som är[29] passiva parter kan anta av samband mellan något anna… ändamål för vilket uppgifterna ursprungligen samlades in (dvs… betaltjänstleverantörer endast behöver den passiva partens uppg… den andra avtalsparten), de berörda[30], det förhållandet att registr… inte rimligen kan förvänta sig ytterligare behandling eller … personuppgiftsansvarig som kan komma att behandla deras perso… de rättsliga begränsningar av behandlingen som föreskrivs i artikel 67.2 f i andra betaltjänstdirektivet.

[29] I skäl 87 i andra betaltjänstdirektivet anges att direktivet endast gäller … mellan betaltjänstanvändaren och dennes betaltjänstleverantör. Andra be… tillämpligt på uppgifter från passiva parter.
[30] Särskild hänsyn ska tas vid behandling av personuppgifter av finansiell … anses öka de eventuella riskerna för enskildas rättigheter och friheter, e… 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 filosofis fackförening och behandling av genetiska uppgifter, biometris identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexuella läggning vara förbjuden.

52. Det bör framhållas att elektroniska betalningar redan är all medlemsstater och att många människor föredrar digital framför transaktioner. Samtidigt kan finansiella transaktioner avslöja k registrerad, inbegripet sådan som hänför sig till särskilda ka grundval av transaktionsuppgifter kan donationer till politiska partier eller organisatione eller församlingar exempelvis avslöja politiska uppfattningar Medlemskap i fackförbund kan avslöjas genom att en årlig medl bankkonto. Genom att analysera fakturor för sjukvård som en registrerad har (t.ex. en psykiater) är det möjligt att samla in personuppgifte information om vissa inköp ge information om en persons sexual framgår av dessa exempel kan till och med enskilda transaktione personuppgifter. Vidare kan kontoinformationstjänster bygga på i artikel 4.4 i dataskyddsförordningen. I artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt godkänts av dataskyddsstyrelsen, kan [p]rofilering [&] skapa s genom att dra slutsatser och kombinera uppgifter som inte utgör en s uppgifter[31]. Detta innebär att de sammantagna finansiella transakti beteendemönster, vilket kan omfatta särskilda kategorier av pers stora att en tjänsteleverantör som behandlar information om transaktioner även behandlar särskilda kategorier av personupp

53. Vad gäller begreppet känsliga betalningsuppgifter noterar sty känsliga betalningsuppgifter i andra betaltjänstdirektivet skiljer s känsliga personuppgifter normalt sätt används i samband med (lagstiftningen om) uppgiftsskydd. Medan andra betaltjänstdi betalningsuppgifter som uppgifter, inbegripet personliga säke kan användas för bedrägerier, framhävs i dataskyddsförordning särskilda kategorier av personuppgifter i artikel 9 i dataskyddsförordningen är särskilt känsliga med hänsyn till grundläggande rättigheter kategorier av personuppgifter[32]. I detta hänseende rekommenderar styrelsen ska kartläggas och kategoriseras vilken typ av personuppgifter som Med största sannolikhet krävs det en konsekvensbedömning avse i dataskyddsförordningen, vilket kommer att vara till hjälp vid de om sådana konsekvensbedömningar finns i artikel 29-gruppens riktlinjer om

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

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

konsekvensbedömning avseende dataskydd och fastställande
sannolikt leder till en hög risk i den mening som avses i förord
styrelsen.

5.2 Möjliga undantag

54. Förbudet i artikel 9 i dataskyddsförordningen är inte absolut.
undantagen i artikel 9.2 i dataskyddsförordningen inte är tillämplig
personuppgifter i samband med andra betaltjänstdirektivet, skulle särskilt föl
artikel 9.2 i dataskyddsförordningen kunna beaktas:

a) Förbudet är inte tillämpligt om den registrerade har lämnat uttry
dessa personuppgifter för ett eller flera specifika ändamål (artik
dataskyddsförordningen).

b) Förbudet är inte tillämpligt om behandlingen är nödvändig av
intresse, på grundval av unionsrätten eller medlemsstaternas
proportion till det eftersträvade syftet, vara förenligt med det
dataskydd och innehålla bestämmelser om lämpliga och särskild
registrerades grundläggande rättigheter och intressen (artikel 9.2 g i dataskyddsförordn

55. Det ska påpekas att förteckningen över undantag i artikel 9.2
uttömmande. Tjänsteleverantörer måste räkna med att det är mö
personuppgifter ingår i uppgifter som behandlas för tillhandahålla
tjänster som omfattas av andra betaltjänstdirektivet. Eftersom
dataskyddsförordningen är tillämpligt på dessa tjänsteleverant
säkerställa att ett av undantagen i artikel 9.2 i dataskyddsförordn
bör framhållas att förbudet i artikel 9.1 är tillämpligt om tjänstel
av undantagen är uppfyllda.

5.3 Viktigt allmänt intresse

56. Betalningstjänster får behandla särskilda kategorier av personup
allmänt intresse, men detta gäller enbart om samtliga vi
dataskyddsförordningen är uppfyllda. Detta innebär att behandlin
av personuppgifter ska föreskrivas i ett särskilt undantag till ar
unionsrätten eller medlemsstaternas nationella rätt. Proportion
eftersträvade syftet med behandlingen måste i denna bestämmelse oc
innehålla lämpliga och specifika åtgärder för att garantera de
rättigheter och intressen. Vidare måste denna unionsrättsliga b
medlemsstaternas nationella rätt vara förenlig med det centrala innehålle
Slutligen måste det visas att behandlingen av de särskilda kateg
av hänsyn till ett viktigt allmänt intresse, inbegripet betydelse
Undantaget kan endast tillämpas på betecknade typer av betaltjä
uppfyllda.

5.4 Uttryckligt samtycke

57. Det enda möjliga lagliga undantag som återstår för behandlin
personuppgifter inom tredjepartsleverantörer i situationer där undanta
dataskyddsförordningen inte är tillämpligt är att erhålla uttryc
villkoren för giltigt samtycke i dataskyddsförordningen (riktlinjer 05/2020

om samtycke enligt förordning (EU) 2016/679[33]. Undantaget enligt artikel 9.2 betr
nödvändig för att fullgöra ett avtal som ett undantag till det al
särskilda kategorier av personuppgifter. Parter och medlemsstater som
sådana situationer bör därför undersöka de särskilda... Om inget av undantage
undantagen i led b–j är tillämpliga, är det enda lagliga undantaget fö
uppgifter erhålla uttryckligt samtycke i enlighet med villkoren för
uttryckligt samtycke enligt artikel 9.2 a i dataskyddsförordning
nämnda förordning är uppfyllda.

5.5 Situationer när det saknas ett tillämpligt undantag

58. Såsom angetts ovan är förbudet i artikel 9.1 tillämpligt om tjäns
av undantagen föreligger. I detta fall kan tekniska åtgärder vidt
särskilda kategorier av personuppgifter, till exempel genom att förhindra behand
uppgifter. I detta avseende kan betaltjänstleverantörer undersö
utesluta särskilda kategorier av personuppgifter och tillåta en u
behandling från tredjepartsleverantörer av särskilda kategorier av p
till passiva parter.

[33] Dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (

6 UPPGIFTSMINIMERING, SÄKERHET, ÖPPENHET, ANSVARSSKYLDIGHET OCH PROFILERING

6.1 Uppgiftsminimering samt inbyggt dataskydd och data

59. Principen om uppgiftsminimering erkänns i artikel 5.1 c i datasky föreskrivs: Personuppgifterna bör vara adekvata, relevanta oc nödvändigt för de ändamål som de behandlas för. Enligt principen personuppgiftsansvariga inte behandla fler personuppgifter än uppnå det särskilda ändamålet. Såsom påpekas i kapitel 2 är de förstådda ändamålet med avtalet och arten av personuppgi nödvändiga för att tillhandahålla betaltjänsten[34]. Principen om uppgiftsminimering är all behandling (dvs. varje insamling av eller tillgång till och dataskyddsstyrelsens riktlinjer Guidelines 4/2019 on Article 25 Data Protectio Default (riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som anges följande: processors and technology providers are also DPbDD, they should also be aware that controllers are required systems and technologies that have built in data protection[35]

60. I artikel 25 i dataskyddsförordningen föreskrivs en skyldighet a dataskydd som standard. Dessa skyldigheter är särskilt v uppgiftsminimering. I denna artikel fastställs att personupp fastställandet av vilka medel behandlingen ska utföras med och vid lämpliga tekniska och organisatoriska åtgärder, vilka är utforma av dataskyddsprinciper och för integrering av de nödvändiga sky att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter personuppgiftsansvarige ska genomföra lämpliga tekniska och o standardfallet, säkerställa att endast personuppgifter som är ändamål med behandlingen behandlas. Den skyldigheten gäller m personuppgifter, behandlingens omfattning, tiden för deras lagri åtgärder kan omfatta kryptering, pseudonymisering och andra te

61. När skyldigheten i artikel 25 i dataskyddsförordningen tillämpas ska genomförandekostnaderna och behandlingens art, omfattning, sa riskerna, av varierande sannolikhetsgrad och allvar, för fysiska beaktas. Denna skyldighet specificeras ytterligare i dataskydd inbyggt dataskydd och dataskydd som standard enligt artikel 25,

6.2 Åtgärder för uppgiftsminimering

62. De tredjepartsleverantörer som får tillgång till betalkontouppgifter för a begärda tjänsterna måste även beakta principen om uppgiftsmin personuppgifter som är nödvändiga för att tillhandahålla de betaltjänstanvändaren begärt. I princip ska tillgången till personu nödvändigt för att tillhandahålla betaltjänster. Såsom har påpe betaltjänstdirektivet en skyldighet för kontoförvaltande betaltjä

[34] Dataskyddsstyrelsens riktlinjer 2/2019 om behandling av personuppgifter dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster
[35] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

av betaltjänstanvändarens information på dennes begäran om be…
en betalningsinitieringstjänst eller en kontoinformationstjänst.

63. Om inte alla betalkontouppgifter är nödvändiga för avtalet bör leverantören av kontoinformationstjänsten välja ut de relevanta uppgiftskategori… Kategorier av uppgifter som inte är nödvändiga kan exempelvis… identitet och transaktionen. Varken mottagarens bankkontonummer eller IBAN från den passiva pa… bankkonto anges, såvida detta inte krävs enligt medlemsstaterna…

64. I detta hänseende kan en eventuell tillämpning av tekniska åtgä… tredjepartsleverantörer när det gäller deras skyldighet att endas… personuppgifter som är nödvändiga för tillhandahållandet av der… genomförandet av lämpliga strategier för dataskydd enligt artikel 24.2 i… dataskyddsförordningen. För att stödja leverantörer av konto… skyldighet att endast samla in personuppgifter som är nödvän… behandlas för rekommenderar styrelsen en katalogisering av… Om… tjänsteleverantör exempelvis inte behöver ha kännedom om vilke… om (i det beskrivande fältet i transaktionsregistret) för att tillh… urvalsverktyg fungera som ett medel för tredjepartsleverantören för att utesluta d… deras sammantagna behandling.

Exempel 2:

HappyPayments, leverantören av kontotjänster från exem… endast behandlar de personliga betalkontouppgifter som a… inte nödvändigt för tillhandahållandet av tjänsten att be… Därför ger företaget användarna möjlighet att välja vil… intresserade av.

Användare A vill ha en överblick över sina utgifter under d… efterfrågar A information om alla transaktioner und… transaktionsbeloppet, datumet för utförandet och mottag… två olika kontoförvaltande betaltjänstleverantörer och… HappyPayments användargränssnitt.

HappyPayments begär sedan endast den information f… betaltjänstleverantörerna som motsvarar de fält som användare A har kryss… senaste två månaderna. Företaget begär inte informa… överföringen eller till och med IBAN, eftersom användare…

För att HappyPayments ska kunna uppfylla sina skyldigheter v… företaget begära tillgång till särskilda fält för en r… betaltjänstleverantörerna.

65. I detta hänseende ska det även noteras att kontoförvaltande bet… tillgång till betaltjänstinformation enligt andra betaltjänstdirek… utgör inte någon rättslig grund för att personuppgifter från andra konto… sparande, lån eller investeringskonton. Således måste teknisk… betaltjänstdirektivet för att säkerställa att tillgången är begräns… som är nödvändig.

66. Förutom att samla in så lite uppgifter som möjligt är tjänstele… genomföra begränsade lagringsperioder. Tjänsteleverantören b…

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

67. Om avtalet mellan den registrerade och leverantören av kont
överföring av personuppgifter till tredje man får endast de perso
fullgörandet av avtalet överföras. Registreraden bör även erhålla särskild i
överföringen och de personuppgifter som ska överföras till denn

6.3 Säkerhet

68. Styrelsen har redan framhållit att åsidosättandet av finansiell
allvarliga konsekvenser för den registrerades dagliga liv och som exemp
betalningsbedrägeri.[36]

69. Om en personuppgiftsincident omfatta finansiella uppgifter kan
betydande risker. Beroende på vilken information som har läckt kan registrerade utsättas
för identitetskapning och att medel på deras konton och andra ti
att exponeringen av transaktionsuppgifter medför betydande r
eftersom transaktionsuppgifter kan innehålla hänvisningar till alla möjlig
registrerades privatliv. Samtidigt är det uppenbart att finansi
brottslingar och därför utgör ett attraktivt mål.

70. Betaltjänstleverantörer är i egenskap av personuppgiftsansvariga skyldiga att vid
åtgärder för att skydda de registrerades personuppgifter (artike
Ju högre risker som är kopplade till den personuppgiftsansva
säkerhetsstandarder behöver tillämpas. Eftersom behandlingen av finansi
rad olika allvarliga risker bör säkerhetsåtgärderna således vara

71. Tjänsteleverantörer bör uppfylla höga standarder, inbegripe
kundautentiseringsförfaranden och höga säkerhetsnivåer för teknisk utrustning[37]. Vidare är även andr
förfaranden viktiga, såsom granskning av personuppgiftsbiträde
och införande av förfaranden mot obehörig tillgång.

6.4 Öppenhet och ansvar

72. Öppenhet och ansvarsskyldighet är centrala principer i dataskyddsförordningen

73. Vad gäller öppenhet (artikel 5.1 a i dataskyddsförordningen
dataskyddsförordningen att personuppgiftsansvariga ska vidta
tillhandahålla all information som avses i artiklarna 13 och 14 i dataskydds
krävs det att informationen eller kommunikationen beträffande b
ska vara i en koncis, klar och tydlig, begriplig och lätt tillgängli
och tydligt språk samt skriftlig eller i någon annan form, inbegr
form. Artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU)
av dataskyddsstyrelsen, ger vägledning om särskilt iakttagande av öppenhe
digitala miljöer.

74. Enligt ovannämnda riktlinjer om öppenhet enligt förordning (E
dataskyddsförordningen tolkas som ett sätt att genomföra en g

[36] Artikel 29-gruppens riktlinjer om konsekvensbedömning avseende dataskydd och fastställa
behandlingen sannolikt leder till en hög risk i den mening som avses i f
som godkänts av styrelsen.
[37] Se de tekniska tillsynsstandarderna.

mentaun att hindra utövandet av den registrerades rättigheter
rättigheter ska möjliggöras med hjälp av kompletterande uppgif
registrerade. Det kan finnas situationer där
som inte innebär att den registrerade måste identifieras (t.ex.
sådana fall kan artikel 11.1 också vara relevant, eftersom
personuppgiftsansvarige inte ska
information för att identifiera den registrerade enbart för att föl

75. Vad gäller tjänsterna enligt andra betaltjänstdirektivet är artik
tillämplig på de
personuppgifter inte har erhållits från den registrerade.

76. I synnerhet ska den registrerade erhålla information om
personuppgifterna kommer att
att fastställa denna period och, i tillämpliga fall, den personup
tredje parts berättigade intressen. Om behandlingen grundas på
dataskyddsförordningen eller uttryckligt samtycke enligt artikel 9.2
krävs det att den registrerade informeras om rätten att när som

77. Den personuppgiftsansvarige ska lämna
särskilda omständigheter under vilka personuppgifterna behand
användas för kommunikation med
leverantörer av kontoinformationstjänster,
tidpunkten för den första kommunikationen med den registrera
lämnas ut till en annan mottagare ska informationen tillhandahål
lämnas ut för första gången.

78. När det
kan tillämpa en skiktad metod där de väljer att använda en ko
säkerställa öppenhet. Det rekommenderas framför a
integritetspolicyer/integritetsmeddelanden bör användas för att län
information som måste ges till de registrerade, i stället för att
samma meddelande på skärmen. Syftet med
samtidigt som det säkerställs att informationen är effektiv.

79. I ovannämnda riktlinjer klargörs även att personuppgiftsansvarig
verktyg för att tillhandahålla enskilda
sekretesspanel kan de registrerade ta del av integritetsin
integritetsrelaterade önskemål genom att tillåta eller förhindra a
på vissa sätt av den personuppgiftsansvarige
de tredjepartsleverantörer som har erhållit uttryckligt samtycke
även erbjuda relevant information om arten och mängden

[38] Artikel 14.3 a i dataskyddsförordningen.
[39] Enligt artikel 29-gruppens riktlinjer om öppenhet enligt förordning (EU) 201
dataskyddsstyrelsen, är sekretesspaneler särskilt användbara när de regis
olika utrustningar, eftersom
använder tjänsten. Genom att ge de registrerade möjlighet att anpassa
sekretesspanel kan man lättare individanpassa integritetsmeddelanden
ange de behandlingstyper som är relevanta för den registrerade.

tredjepartsleverantörer har tillgång till. I princip kan en kontoförvaltande
erbjuda användaren en möjlighet att återkalla särskilt uttryc
betaltjänstdirektivet[40] genom denna överblick, vilket skulle medföra nek
betalkonton för en eller flera tredjepartleverantörer. Användar
kontoförvaltande betaltjänstleverantör nekar tillgång till deras
särskilda tredjepartsleverantörer[41], eftersom användaren har rätt att använda (en
kontoinformationstjänst. Om sekretesspaneler används för att lä
samtycke bör de utformas och tillämpas på ett lagligt sätt och
hinder mot tredjepartleverantörernas rätt att tillhandahålla tjänster i enlighet m
betaltjänstdirektivet. I detta hänseende och i enlighet med de ti
betaltjänstdirektivet har en tredjepartsleverantör möjlighet att p
från användaren efter det att detta samtycke har återkallats.

80. Enligt ansvarsprincipen är den personuppgiftsansvarige skyldig
organisatoriska åtgärder för att säkerställa och kunna visa att b
dataskyddsförordningen, i synnerhet i överensstämmelse med de
dataskydd som föreskrivs i artikel 5.1. I samband med dessa å
omfattning, sammanhang och ändamål beaktas samt riskerna för fy
friheter och de ska ses över och uppdateras vid behov[42].

6.5 Profilering

81. Betaltjänstleverantörernas behandling av personuppgifter kan in
4.4 i dataskyddsförordningen. Till exempel kan leverantörer av k
sig av automatisk behandling av personuppgifter för att bedöma vissa pers
aspekter. En registrerads finansiella situation kan bedömas, b
innehåll. Kontoinformationstjänster som ska tillhandahållas på a
en omfattande bedömning av betalkontouppgifter.

82. Den personuppgiftsansvarige ska även vara öppen mot den
förekomsten av automatiserat beslutsfattande, inbegripet prof
personuppgiftsansvarige lämna meningsfull information om logiken bakom samt betydels
de förutsedda följderna av sådan behandling för den registrerad
skäl 60[43]. Enligt artikel 15 i dataskyddsförordningen har den regis
erhålla information från den personuppgiftsansvarige om förekomsten
beslutsfattande, inbegripet profilering, logiken bakom samt bety
under vissa förutsättningar, en rätt att göra invändningar mot pr
enbart är frågan om automatiserat individuellt beslutsfattande[44] s

83. Vidare är rätten för den registrerade att inte bli föremål för et
automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller
eller på liknande sätt i betydande grad påverkar honom eller he
dataskyddsförordningen relevant i detta sammanhang. Denna bes

---

[40] Se, till exempel, det uttryckliga godkännande till vilket hänvisas i arti
[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,
dataskyddsstyrelsen.
[44] Artikel 29-gruppen riktlinjer om automatiserat individuellt beslutsfattande oc
(EU) 2016/679, WP251, rev.01.

vissa omständigheter, en skyldighet för personuppgiftsansvariga att genomföra
för att skydda den registrerades rättigheter, såsom särskild infor
till personlig kontakt vid beslutsfattandet och att kunna uttrycka
Såsom även anges i skäl 71 i dataskyddsförordningen innebär de
bör ha rätt att inte bli föremål för ett beslut, såsom ett automat
online utan personlig kontakt.[45]

84. Automatiserat beslutsfattande, inbegripet profilering, som inbegriper personuppgifter är endast tillåtet om följande kumulativa dataskyddsförordningen är uppfyllda:

- Ett undantag enligt artikel 22.2 kan tillämpas.
- Artikel 9.2 a eller g i dataskyddsförordningen är tillämplig. personuppgiftsansvarige vidta lämpliga åtgärder för att skydd och friheter och berättigade intressen.[46]

85. Vidare ska även de krav på behandling som anges i dessa riktlinjer Förtydligandena och anvisningarna om automatiserat individuellt artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfa förordning (EU) 2016/679 som godkänts av dataskyddsstyrelsen är i h 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 o (EU) 2016/679, WP251, rev.01, sidan 24.