Retningslinjer 06/2020 om samspillet mellem andet betalingstjenestedirektiv og databeskyttelsesforordningen

Version 2.0

Vedtaget den 15. december 2020

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

Versionshistorik

Version 2.0	15.12.2020	Vedtagelse af retningslinjerne efter offentlig høring
Version 1.0	17.7.2020	Vedtagelse af retningslinjerne med henblik på offentlig høring

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet") har —

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter benævnt "databeskyttelsesforordningen"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018[1],

under henvisning til artikel 12 og 22 i Databeskyttelsesrådets forretningsorden,

ud fra følgende betragtninger:

(1) Databeskyttelsesforordningen fastsætter et ensartet regelsæt for behandling af personoplysninger i hele EU.

(2) Det andet betalingstjenestedirektiv (Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 23. december 2015) ophæver direktiv 2007/64/EF og fastsætter nye regler for at sikre retssikkerheden for forbrugere, handlende og virksomheder i betalingskæden og modernisere de retlige rammer for markedet for betalingstjenester[2]. Medlemsstaterne skulle gennemføre det andet betalingstjenestedirektiv i deres nationale lovgivning inden den 13. januar 2018.

(3) Et vigtigt træk ved det andet betalingstjenestedirektiv er indførelsen af en retlig ramme for nye betalingsinitieringstjenester og kontooplysningstjenester. Det andet betalingstjenestedirektiv giver disse nye betalingstjenesteudbydere mulighed for at få adgang til de registreredes betalingskonti med henblik på at levere de pågældende tjenester.

(4) For så vidt angår databeskyttelse skal enhver behandling af personoplysninger, herunder tilvejebringelse af oplysninger om behandlingen, med henblik på det andet betalingstjenestedirektiv i overensstemmelse med artikel 94, stk. 1, i det andet betalingstjenestedirektiv, foretages i overensstemmelse med databeskyttelsesforordningen[3] og forordning (EU) 2018/1725.

(5) I betragtning 89 i det andet betalingstjenestedirektiv anføres det, at når personoplysninger behandles med henblik på det andet betalingstjenestedirektiv, bør det præcise formål med behandlingen angives, det gældende retsgrundlag bør anføres, de relevante sikkerhedskrav i databeskyttelsesforordningen bør gennemføres, og principperne om nødvendighed, proportionalitet, formålsbegrænsning og rimelige dataopbevaringsperioder skal overholdes. Desuden bør databeskyttelse gennem design og standardindstillinger integreres i alle databehandlingssystemer, der udvikles og anvendes inden for rammerne af det andet betalingstjenestedirektiv[4].

(6) I betragtning 93 i det andet betalingstjenestedirektiv anføres det, at betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere på den ene side og den

[1] Henvisninger til "medlemsstater" i hele dette dokument skal forstås som henvisninger til "EØS-medlemsstater".
[2] Betragtning 6 i det andet betalingstjenestedirektiv.
[3] Da det andet betalingstjenestedirektiv er ældre end databeskyttelsesforordningen, henviser det stadig til direktiv 95/46. Artikel 94 i databeskyttelsesforordningen fastsætter, at henvisninger til det ophævede direktiv 95/46 skal betragtes som henvisninger til databeskyttelsesforordningen.
[4] Betragtning 89, det andet betalingstjenestedirektiv.

kontoførende betalingstjenesteudbyder på den anden side bør overholde de nødvendige databeskyttelses- og sikkerhedskrav, der er fastsat eller henvist til i dette direktiv eller medtaget i de reguleringsmæssige tekniske standarder.

HAR VEDTAGET FØLGENDE RETNINGSLINJER

1. INDLEDNING

1. Med det andet betalingstjenestedirektiv er der indført en række nye tiltag inden for betalingstjenester. Selv om det skaber nye muligheder for forbrugerne og øger gennemsigtigheden på dette område, rejser anvendelsen af det andet betalingstjenestedirektiv visse spørgsmål og bekymringer med hensyn til behovet for, at de registrerede fortsat har fuld kontrol over deres personoplysninger. Databeskyttelsesforordningen finder anvendelse på behandling af personoplysninger, herunder behandlingsaktiviteter i forbindelse med betalingstjenester som defineret i det andet betalingstjenestedirektiv[5]. Dataansvarlige, der handler på det område, der er omfattet af det andet betalingstjenestedirektiv, skal derfor altid sikre overholdelse af kravene i databeskyttelsesforordningen, herunder principperne om databeskyttelse i artikel 5 i databeskyttelsesforordningen, samt de relevante bestemmelser i e-databeskyttelsesdirektivet[6]. Selv om det andet betalingstjenestedirektiv[7] og de reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation (i det følgende benævnt "reguleringsmæssige tekniske standarder"[8]) indeholder visse bestemmelser vedrørende databeskyttelse og sikkerhed, er der opstået usikkerhed om fortolkningen af disse bestemmelser samt samspillet mellem den generelle databeskyttelsesramme og det andet betalingstjenestedirektiv.

2. Den 5. juli 2018 udsendte Databeskyttelsesrådet en skrivelse vedrørende det andet betalingstjenestedirektiv, hvori Databeskyttelsesrådet redegjorde for spørgsmål vedrørende beskyttelse af personoplysninger i forbindelse med det andet betalingstjenestedirektiv, navnlig om kontooplysningstjenesteudbyderes og betalingsinitieringstjenesteudbyderes behandling af personoplysninger om ikkekontraherende parter (såkaldte "data fra passive interessenter"), procedurerne for afgivelse og tilbagetrækning af samtykke, den pålidelige overførselstjeneste og samarbejdet mellem kontoførende betalingstjenesteudbydere, reguleringsmæssige tekniske standarder og samarbejdet mellem kontoførende betalingstjenesteudbydere i forbindelse med sikkerhedsforanstaltninger. Det forberedende arbejde med disse retningslinjer omfattede indsamling af input fra interessenter, både skriftligt og ved et arrangement med interessenter, med henblik på at identificere de mest presserende udfordringer.

[5] Databeskyttelsesforordningen, artikel 1, stk. 1.

[6] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation), EUT L 201 AF 31/07/2002 s. 0037-0047.

[7] Artikel 94 i betalingstjenestedirektivet osv.

[8] Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation (EØS-relevant tekst.) C/2017/7782, EUT L 69 af 13.3.2018, s. 23-43, findes på https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN.

3. Disse retningslinjer har til formål at give yderligere vejledning om databeskyttelsesaspekter i forbindelse med det andet betalingstjenestedirektiv, navnlig om forholdet mellem relevante bestemmelser om databeskyttelsesforordningen og det andet betalingstjenestedirektiv. Disse retningslinjer fokuserer primært på kontooplysningstjenesteudbyderes og betalingsinitieringstjenesteudbyderes behandling af personoplysninger. Dette dokument omhandler således betingelserne for at give kontoførende betalingstjenesteudbydere adgang til oplysninger om betalingskonti og for betalingsinitieringstjenesteudbyderes og kontooplysningstjenesteudbyderes behandling af personoplysninger, herunder krav og garantier i forbindelse med betalingsinitieringstjenesteudbyderes og kontooplysningstjenesteudbyderes behandling af personoplysninger til andre formål end de oprindelige formål, hvortil oplysningerne er indsamlet, navnlig når de er indsamlet i forbindelse med levering af en kontooplysningstjeneste[9]. Dette dokument omhandler også forskellige opfattelser af udtrykkeligt samtykke i henhold til det andet betalingstjenestedirektiv og databeskyttelsesforordningen, behandlingen af "data fra passive interessenter", betalingsinitieringstjenesteudbyderes og kontooplysningstjenesteudbyderes behandling af særlige kategorier af personoplysninger, anvendelsen af de vigtigste databeskyttelsesprincipper i databeskyttelsesforordningen, herunder dataminimering, gennemsigtighed, ansvarlighed og sikkerhedsforanstaltninger. Det andet betalingstjenestedirektiv indebærer tværgående ansvarsområder inden for bl.a. forbrugerbeskyttelse og konkurrenceret. Overvejelser vedrørende disse lovgivningsområder ligger uden for rammerne af disse retningslinjer.

4. For at lette læsningen af retningslinjerne er de vigtigste definitioner i dette dokument anført nedenfor.

1.1 Definitioner

"Kontooplysningstjenesteudbyder": udbyderen af en onlinetjeneste, der leverer konsoliderede oplysninger om en eller flere betalingskonti, som betalingstjenestebrugeren er indehaver af hos enten en anden betalingstjenesteudbyder eller hos flere end én betalingstjenesteudbyder.

"Kontoførende betalingstjenesteudbyder": en betalingstjenesteudbyder, der stiller en betalingskonto til rådighed og fører en betalingskonto for en betaler.

"Dataminimering": et princip om databeskyttelse, ifølge hvilket personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

"Betaler": en fysisk eller juridisk person, der er indehaver af en betalingskonto og tillader en betalingsordre fra denne betalingskonto, eller, hvis der ikke er nogen betalingskonto, en fysisk eller juridisk person, der udsteder en betalingsordre.

"Betalingsmodtager": en fysisk eller juridisk person, som er den tiltænkte modtager af de midler, der indgår i en betalingstransaktion.

"Betalingskonto": en konto oprettet i en eller flere betalingstjenestebrugeres navn med henblik på at gennemføre betalingstransaktioner.

[9] En kontooplysningstjeneste er en onlinetjeneste, der leverer konsoliderede oplysninger om en eller flere betalingskonti, som betalingstjenestebrugeren er indehaver af hos enten en anden betalingstjenesteudbyder eller hos flere end én betalingstjenesteudbyder.

"Betalingsinitieringstjenesteudbyder": udbyderen af en tjeneste til initiering af en betalingsordre på betalingstjenestebrugerens anmodning for en betalingskonto hos en anden betalingstjenesteudbyder.

"Betalingstjenesteudbyder": et organ, som omhandlet i artikel 1, stk. 1, i det andet betalingstjenestedirektiv[10], eller en fysisk eller juridisk person, der er omfattet af en undtagelse i henhold til artikel 32 eller 33 i det andet betalingstjenestedirektiv.

"Betalingstjenestebruger": en fysisk eller juridisk person, som bruger en betalingstjeneste som betaler eller betalingsmodtager eller begge dele.

"Personoplysninger": enhver form for information om en identificeret eller identificerbar fysisk person ("den registrerede"). Ved "identificerbar fysisk person" forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

"Databeskyttelse gennem design": tekniske og organisatoriske foranstaltninger, der er integreret i et produkt eller en tjeneste, og som er udformet med henblik på at gennemføre databeskyttelsesprincipper på en effektiv måde og integrere de nødvendige garantier i behandlingen for at opfylde kravene i databeskyttelsesforordningen og beskytte registreredes rettigheder.

"Databeskyttelse gennem indstillinger": passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles.

Reguleringsmæssige tekniske standarder: Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation.

"Tredjepartsudbydere" henviser til både betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere.

1.2 Tjenester i henhold til det andet betalingstjenestedirektiv

[10] Det fremgår af artikel 1, stk. 1, i det andet betalingstjenestedirektiv, at det andet betalingstjenestedirektiv fastsætter regler, i henhold til hvilke medlemsstaterne skal sondre mellem følgende kategorier af *betalingstjenesteudbydere*:
a) kreditinstitutter som defineret i artikel 4, stk. 1, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013, herunder filialer heraf som defineret i den i nævnte forordnings artikel 4, stk. 1, nr. 17), når sådanne filialer er beliggende i Unionen, hvad enten disse filialers hovedkontorer er beliggende i Unionen eller, i overensstemmelse med artikel 47 i direktiv 2013/36/EU og national ret, uden for Unionen
b) e-pengeinstitutter som defineret i artikel 2, nr. 1), i direktiv 2009/110/EF, herunder, i overensstemmelse med artikel 8 i nævnte direktiv og med national ret, filialer heraf, hvis sådanne filialer er beliggende i Unionen, og deres hovedkontor er beliggende uden for Unionen, i det omfang de betalingstjenester, som udbydes af disse filialer, har forbindelse til udstedelse af elektroniske penge
c) postgirokontorer, der i henhold til national lovgivning har ret til at udbyde betalingstjenester
d) betalingsinstitutter
e) ECB og nationale centralbanker, når de ikke handler i deres egenskab af pengepolitiske myndigheder eller andre offentlige myndigheder
f) medlemsstater eller deres regionale og lokale myndigheder, når de ikke handler i deres egenskab af offentlige myndigheder.

5. Med det andet betalingstjenestedirektiv indføres der to nye former for betalingstjenester (udbydere): Betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere. Bilag 1 til det andet betalingstjenestedirektiv indeholder de otte betalingstjenester, der er omfattet af det andet betalingstjenestedirektiv.

6. Betalingsinitieringstjenesteudbydere udbyder tjenester til initiering af betalingsordrer på betalingstjenestebrugerens anmodning for en brugers betalingskonto hos en anden betalingstjenesteudbyder[11]. En betalingsinitieringstjenesteudbyder kan anmode en kontoførende betalingstjenesteudbyder (normalt en bank) om at initiere en transaktion på vegne af betalingstjenestebrugeren. Betalingstjenestebrugeren kan være en fysisk person (registreret person) eller en juridisk person.

7. Kontooplysningstjenesteudbydere leverer onlinetjenester i forbindelse med konsoliderede oplysninger om en eller flere betalingskonti, som betalingstjenestebrugeren er indehaver af hos enten en anden betalingstjenesteudbyder eller hos flere end én betalingstjenesteudbyder[12]. I henhold til 28. betragtning til det andet betalingstjenestedirektiv kan betalingstjenestebrugeren straks få et samlet overblik over sin finansielle situation på et givet tidspunkt.

8. Når det drejer sig om kontooplysningstjenester, kan der tilbydes flere forskellige typer tjenester med vægt på forskellige karakteristika og formål. Nogle udbydere kan f.eks. tilbyde brugertjenester såsom budgetplanlægning og overvågning af udgifter. Behandlingen af personoplysninger i forbindelse med disse tjenester er omfattet af det andet betalingstjenestedirektiv. Tjenester, der indebærer vurderinger af betalingstjenestebrugerens kreditværdighed, eller revisionstjenester, der udføres på grundlag af indsamling af oplysninger via en kontooplysningstjeneste, falder uden for anvendelsesområdet for det andet betalingstjenestedirektiv, og falder derfor ind under databeskyttelsesforordningen. Desuden er andre konti end betalingskonti (f.eks. opsparing, investering) heller ikke omfattet af det andet betalingstjenestedirektiv. Under alle omstændigheder er databeskyttelsesforordningen den gældende retlige ramme for behandling af personoplysninger.

Eksempel 1:
HappyPayments er en virksomhed, der tilbyder en onlinetjeneste, som består i at stille oplysninger om en eller flere betalingskonti til rådighed via en mobilapp med henblik på finansielt tilsyn (en kontooplysningstjeneste). Med denne tjeneste kan betalingstjenestebrugeren se saldi og nylige transaktioner på to eller flere betalingskonti i forskellige banker. Den tilbyder også, når en betalingstjenestebruger vælger at benytte det, en kategorisering af udgifter og indtægter efter forskellige typologier (løn, fritid, energi, realkreditlån osv.), hvilket hjælper betalingstjenestebrugeren med den finansielle planlægning. I denne app tilbyder HappyPayments også en tjeneste til at initiere betalinger direkte fra en eller flere af brugerens angivne betalingskonti (en betalingsinitieringstjeneste).

9. Med henblik på at levere disse tjenester regulerer det andet betalingstjenestedirektiv de retlige betingelser, hvorunder betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere kan få adgang til betalingskonti for at levere en tjeneste til betalingstjenestebrugeren.

10. Artikel 66, stk. 1, og artikel 67, stk. 1, i det andet betalingstjenestedirektiv fastsætter, at adgang til og brug af betalings- og kontooplysningstjenester er betalingstjenestebrugerens rettigheder. Dette

[11] Artikel 4, stk. 15, i det andet betalingstjenestedirektiv.
[12] Artikel 4, stk. 16, i det andet betalingstjenestedirektiv.

betyder, at betalingstjenestebrugeren bør forblive fuldstændig fri med hensyn til udøvelsen af denne ret og ikke kan tvinges til at gøre brug af denne ret.

11. Adgang til betalingskonti og anvendelse af betalingskontooplysninger er delvist reguleret i artikel 66 og 67 i det andet betalingstjenestedirektiv, som indeholder sikkerhedsforanstaltninger vedrørende beskyttelse af data (personoplysninger). I henhold til artikel 66, stk. 3, litra f), i det andet betalingstjenestedirektiv må betalingsinitieringstjenesteudbyderen ikke anmode betalingstjenestebrugeren om andre data end dem, der er nødvendige for at levere betalingsinitieringstjenesten, og artikel 66, stk. 3, litra g), i det andet betalingstjenestedirektiv fastsætter, at betalingsinitieringstjenesteudbydere ikke må anvende, tilgå eller lagre data til andre formål end at udføre den betalingsinitieringstjeneste, som betalingstjenestebrugeren udtrykkeligt har anmodet om. Endvidere begrænser artikel 67, stk. 2, litra d), i det andet betalingstjenestedirektiv adgangen for kontooplysningstjenesteudbydere til oplysninger fra udpegede betalingskonti og tilhørende betalingstransaktioner, mens artikel 67, stk. 2, litra f), i det andet betalingstjenestedirektiv fastsætter, at kontooplysningstjenesteudbydere ikke må anvende, tilgå eller lagre data til andre formål end at udføre den kontooplysningstjeneste, som betalingstjenestebrugeren udtrykkeligt har anmodet om, i overensstemmelse med databeskyttelsesreglerne. Sidstnævnte understreger, at personoplysninger inden for rammerne af kontooplysningstjenesterne kun må indsamles til udtrykkeligt angivne og legitime formål. En kontooplysningstjenesteudbyder skal derfor i kontrakten udtrykkeligt angive, til hvilke specifikke formål personkontooplysningerne vil blive behandlet i forbindelse med den kontooplysningstjeneste, som kontooplysningstjenesteudbyderen udbyder. Kontrakten skal være lovlig, retfærdig og gennemsigtig i henhold til artikel 5 i databeskyttelsesforordningen, og den skal også overholde andre forbrugerbeskyttelseslove.

12. Afhængigt af specifikke omstændigheder kan betalingstjenesteudbydere være dataansvarlige eller databehandlere i henhold til databeskyttelsesforordningen. I disse retningslinjer forstås ved "dataansvarlige" de betalingstjenesteudbydere, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Der findes yderligere vejledning herom i Databeskyttelsesrådets retningslinjer 07/2020 om begreberne dataansvarlig og databehandler i databeskyttelsesforordningen.

2 LOVLIGE GRUNDE OG YDERLIGERE BEHANDLING I HENHOLD TIL DET ANDET BETALINGSTJENESTEDIREKTIV

2.1 Lovlige grunde til behandling

13. I henhold til databeskyttelsesforordningen skal dataansvarlige have et retsgrundlag for behandling af personoplysninger. Artikel 6, stk. 1, i databeskyttelsesforordningen udgør en udtømmende og afgrænsende liste over seks retsgrundlag for behandling af personoplysninger i henhold til databeskyttelsesforordningen[13]. Det er op til den dataansvarlige at definere det korrekte retsgrundlag og sikre, at alle betingelser for dette retsgrundlag er opfyldt. Fastlæggelsen af, hvilket grundlag der er gyldigt og mest hensigtsmæssigt i en bestemt situation, afhænger af de omstændigheder, hvorunder behandlingen finder sted, herunder formålet med behandlingen og forholdet mellem den dataansvarlige og den registrerede.

2.2 Artikel 6, stk. 1, litra b), i databeskyttelsesforordningen (behandling er nødvendig af hensyn til opfyldelsen af en kontrakt)

14. Betalingstjenester leveres på kontraktbasis mellem betalingstjenestebrugeren og betalingstjenesteudbyderen. Som anført i betragtning 87 i det andet betalingstjenestedirektiv bør "*[dette direktiv] kun vedrøre aftalemæssige forpligtelser og ansvar mellem betalingstjenestebrugeren og betalingstjenesteudbyderen.*" Med hensyn til databeskyttelsesforordningen er det vigtigste retsgrundlag for behandling af personoplysninger med henblik på levering af betalingstjenester artikel 6, stk. 1, litra b), i databeskyttelsesforordningen, hvilket betyder, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, eller for at træffe foranstaltninger på den registreredes anmodning forud for indgåelsen af en kontrakt.

15. Betalingstjenester i henhold til det andet betalingstjenestedirektiv er defineret i bilag 1 til det andet betalingstjenestedirektiv. Leveringen af disse tjenester som defineret i det andet betalingstjenestedirektiv er et krav for indgåelse af en kontrakt, hvorunder parterne har adgang til betalingstjenestebrugerens betalingskontodata. Disse betalingstjenesteudbydere skal også være i

[13] I henhold til artikel 6 er behandling kun lovlig, hvis og i det omfang mindst et af følgende forhold gør sig gældende:

(a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.

(b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.

(c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

(d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.

(e) Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

(f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

besiddelse af en licens. I forbindelse med betalingsinitieringstjenester og kontooplysningstjenester i henhold til det andet betalingstjenestedirektiv kan kontrakter omfatte vilkår, der også pålægger betingelser for yderligere tjenester, som ikke er reguleret af det andet betalingstjenestedirektiv. *Databeskyttelsesrådets retningslinjer 2/2019 om behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i databeskyttelsesforordningen i forbindelse med levering af onlinetjenester til registrerede* gør det klart, at dataansvarlige skal vurdere, hvilken behandling af personoplysninger der er objektivt nødvendig for at opfylde kontrakten. Det påpeges i disse retningslinjer, at begrundelsen for nødvendigheden afhænger af tjenesteydelsens art, kontraktparternes gensidige perspektiver og forventninger, baggrunden for kontrakten og de væsentlige elementer i kontrakten.

16. Databeskyttelsesrådets retningslinjer 2/2019 gør det også klart, at der i lyset af artikel 7, stk. 4, i databeskyttelsesforordningen skelnes mellem behandlingsaktiviteter, der er nødvendige for udførelsen af en kontrakt, og vilkår, der gør tjenesten betinget af visse behandlingsaktiviteter, som faktisk ikke er nødvendige for opfyldelsen af kontrakten. "Nødvendige for opfyldelse" kræver tydeligvis noget mere end en kontraktlig betingelse[14]. Den dataansvarlige bør kunne påvise, hvordan hovedformålet med den specifikke kontrakt med den registrerede rent faktisk ikke kan udføres, hvis den specifikke behandling af de pågældende personoplysninger ikke finder sted. Det er ikke tilstrækkeligt blot at henvise til eller nævne databehandling i en kontrakt for at bringe den pågældende behandling ind under anvendelsesområdet for artikel 6, stk. 1, litra b), i databeskyttelsesforordningen.

17. I artikel 5, stk. 1, litra b), i databeskyttelsesforordningen tages der højde for princippet om formålsbegrænsning, i henhold til hvilket personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål. Ved vurderingen af, om artikel 6, stk. 1, litra b), er et passende retsgrundlag for en onlinetjeneste (betaling), bør der tages hensyn til tjenestens særlige sigte, formål eller mål[15]. Formålene med behandlingen skal være klart angivet og meddelt den registrerede i overensstemmelse med den dataansvarliges formålsbegrænsnings- og gennemsigtighedsforpligtelser. En vurdering af, hvad der er "nødvendigt", indebærer en kombineret, faktabaseret vurdering af behandlingen "til det formål, der forfølges, og om det er mindre indgribende sammenlignet med andre muligheder for at opnå det samme mål". Artikel 6, stk. 1, litra b), omfatter ikke behandling, der er nyttig, men ikke objektivt nødvendig for at udføre den kontraktmæssige tjeneste eller for at tage relevante skridt forud for indgåelsen af kontrakten på den registreredes anmodning, selv om det er nødvendigt af hensyn til den dataansvarliges andre forretningsmæssige formål[16].

18. Databeskyttelsesrådets retningslinjer 2/2019 gør det klart, at kontrakter ikke kunstigt kan udvide de kategorier af personoplysninger eller typer af behandlingsaktiviteter, som den dataansvarlige skal udføre for at opfylde kontrakten, jf. artikel 6, stk. 1, litra b)[17]. Disse retningslinjer omhandler også tilfælde, hvor der kan skabes "take it or leave it"-situationer for registrerede, som måske kun er interesseret i én af tjenesterne. Dette kan ske, hvis en dataansvarlig ønsker at samle flere særskilte tjenester eller elementer af en tjeneste med forskellige grundlæggende formål,

[14] Retningslinjer 2/2019 om behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i databeskyttelsesforordningen i forbindelse med levering af onlinetjenester til registrerede, Databeskyttelsesrådet, s. 8.
[15] Som ovenfor.
[16] Som ovenfor, s. 7.
[17] Som ovenfor, s. 10.

funktioner eller begrundelser i én kontrakt. Hvis kontrakten består af flere særskilte tjenester eller elementer af en tjeneste, som faktisk med rimelighed kan udføres uafhængigt af hinanden, bør anvendelsen af artikel 6, stk. 1, litra b), vurderes særskilt i forbindelse med hver af disse tjenester, idet der ses på, hvad der er objektivt nødvendigt for at udføre hver enkelt af de individuelle tjenester, som den registrerede aktivt har anmodet om eller tilmeldt sig[18].

19. I overensstemmelse med ovennævnte retningslinjer skal de dataansvarlige vurdere, hvad der er objektivt nødvendigt for opfyldelsen af kontrakten. Hvis dataansvarlige ikke kan påvise, at behandlingen af personoplysninger om betalingskonti er objektivt nødvendig for separat levering af hver af disse tjenester, er artikel 6, stk. 1, litra b), i databeskyttelsesforordningen ikke et gyldigt retsgrundlag for behandling. I sådanne tilfælde bør den dataansvarlige overveje et andet retsgrundlag for behandling.

2.3 Forebyggelse af svig

20. I henhold til artikel 94, stk. 1, i det andet betalingstjenestedirektiv skal medlemsstaterne tillade, at betalingssystemer og betalingstjenesteudbydere behandler personoplysninger, når det er nødvendigt for at beskytte forebyggelse, efterforskning og afsløring af betalingssvig. Behandling af personoplysninger, der er strengt nødvendige for at forebygge svig, kan udgøre en legitim interesse for den pågældende betalingstjenesteudbyder, forudsat at den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder ikke går forud herfor[19]. Behandlingsaktiviteter med henblik på forebyggelse af svig bør baseres på en omhyggelig vurdering fra sag til sag foretaget af den dataansvarlige i overensstemmelse med ansvarlighedsprincippet. For at forebygge svig kan dataansvarlige desuden være underlagt specifikke retlige forpligtelser, der nødvendiggør behandling af personoplysninger.

2.4 Yderligere behandling (kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere)

21. Artikel 6, stk. 4, i databeskyttelsesforordningen fastsætter betingelserne for behandling af personoplysninger til et andet formål end det, hvortil personoplysningerne er indsamlet. Mere specifikt kan en sådan yderligere behandling finde sted, hvis den er baseret på EU-retten eller en medlemsstats lovgivning, hvilket udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund for at beskytte de mål, der er omhandlet i artikel 23, stk. 1, hvis den registrerede har givet sit samtykke, eller hvis behandlingen til et andet formål end det, hvortil personoplysningerne blev indsamlet, er forenelig med det oprindelige formål.

22. Der skal tages nøje hensyn til artikel 66, stk. 3, litra g), og artikel 67, stk. 2, litra f), i det andet betalingstjenestedirektiv. Som nævnt ovenfor fremgår det af artikel 66, stk. 3, litra g), i det andet betalingstjenestedirektiv, at betalingsinitieringstjenesteudbyderen ikke må anvende, tilgå eller lagre data til andre formål end levering af betalingsinitieringstjenesten, som betaleren udtrykkeligt har anmodet om. Artikel 67, stk. 2, litra f), i det andet betalingstjenestedirektiv fastsætter, at kontooplysningstjenesteudbyderen ikke må anvende, tilgå eller lagre data til andre formål end at udføre den kontooplysningstjeneste, som betalingstjenestebrugeren udtrykkeligt har anmodet om, i overensstemmelse med databeskyttelsesreglerne.

23. Følgelig begrænser artikel 66, stk. 3, litra g), og artikel 67, stk. 2, litra f), i det andet betalingstjenestedirektiv betydeligt mulighederne for behandling til andre formål, hvilket betyder, at behandling til et andet formål ikke er tilladt, medmindre den registrerede har givet sit samtykke

[18] Som ovenfor, s. 11.
[19] Betragtning 47 i databeskyttelsesforordningen.

i henhold til artikel 6, stk. 1, litra a), i databeskyttelsesforordningen, eller behandlingen er fastsat i EU-retten eller en medlemsstats lovgivning, som den dataansvarlige er underlagt, i henhold til artikel 6, stk. 4, i databeskyttelsesforordningen. Hvis behandlingen til et andet formål end det, hvortil personoplysningerne er indsamlet, ikke er baseret på den registreredes samtykke eller på EU-ret eller en medlemsstats lovgivning, gør de begrænsninger, der er fastsat i artikel 66, stk. 3, litra g), og artikel 67, stk. 2, litra f), i det andet betalingstjenestedirektiv det klart, at et hvilket som helst andet formål ikke er foreneligt med det formål, hvortil personoplysningerne oprindeligt blev indsamlet. Forenelighedstesten i artikel 6, stk. 4, i databeskyttelsesforordningen kan ikke føre til et retsgrundlag for behandling.

24. Artikel 6, stk. 4, i databeskyttelsesforordningen giver mulighed for yderligere behandling på grundlag af EU-retten eller medlemsstaternes lovgivning. For eksempel er alle betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere forpligtede enheder i henhold til artikel 3, stk. 2, litra a), i Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme i henhold til direktivet om bekæmpelse af hvidvaskning af penge. Disse forpligtede enheder er derfor tvunget til at anvende de kundekendskabsprocedurer, der er fastsat i direktivet. De personoplysninger, der behandles i forbindelse med en tjeneste i henhold til det andet betalingstjenestedirektiv, behandles derfor yderligere på grundlag af mindst én retlig forpligtelse for tjenesteudbyderen[20].

25. Som nævnt i stk. 20 fremgår det af artikel 6, stk. 4, i databeskyttelsesforordningen, at behandling til et andet formål end det, hvortil personoplysningerne er indsamlet, kan baseres på den registreredes samtykke, hvis alle betingelserne for samtykke i henhold til databeskyttelsesforordningen er opfyldt. Som anført ovenfor skal den dataansvarlige påvise, at det er muligt at afvise eller tilbagetrække samtykke uden skadelige følger (betragtning 42 i databeskyttelsesforordningen).

2.5 Lovlig grund til at give adgang til kontoen (kontoførende betalingstjenesteudbydere)

26. Som nævnt i punkt 10 kan betalingstjenestebrugere udøve deres ret til at gøre brug af betalingsinitierings- og kontooplysningstjenester. De forpligtelser, der pålægges medlemsstaterne i artikel 66, stk. 1, og artikel 67, stk. 1, i det andet betalingstjenestedirektiv, bør gennemføres i national lovgivning for at sikre en effektiv anvendelse af betalingstjenestebrugerens ret til at drage fordel af de nævnte betalingstjenester. En effektiv anvendelse af sådanne rettigheder ville ikke være mulig uden en tilsvarende forpligtelse for den kontoførende betalingstjenesteudbyder, typisk en bank, til at give betalingstjenesteudbyderen adgang til kontoen på den betingelse, at den har opfyldt alle krav for at få adgang til betalingstjenestebrugerens konto. Endvidere fremgår det klart af artikel 66, stk. 5, og artikel 67, stk. 4, i det andet betalingstjenestedirektiv, at levering af betalingsinitieringstjenester og kontooplysningstjenester ikke må afhænge af, om der foreligger et kontraktforhold mellem betalingsinitieringstjenesteudbyderen/kontooplysningstjenesteudbyderen og den kontoførende betalingstjenesteudbyder.

27. Den kontoførende betalingstjenesteudbyders behandling af personoplysninger, der består i at give adgang til de personoplysninger, som betalingsinitieringstjenesteudbyderen og

[20] Bemærk, at en grundig undersøgelse af spørgsmålet om, hvorvidt hvidvaskningsdirektivet opfylder standarden i artikel 6, stk. 4, i databeskyttelsesforordningen, falder uden for dette dokuments anvendelsesområde.

kontooplysningstjenesteudbyderen anmoder om med henblik på at udføre deres betalingstjeneste over for brugeren af betalingstjenester, er baseret på en retlig forpligtelse. For at opfylde målene for det andet betalingstjenestedirektiv skal kontoførende betalingstjenesteudbydere levere personoplysninger til betalingsinitieringstjenesteudbydernes og kontooplysningstjenesteudbydernes tjenester, hvilket er en nødvendig forudsætning for, at betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere kan levere deres tjenester og dermed sikre de rettigheder, der er fastsat i artikel 66, stk. 1, og artikel 67, stk. 1, i det andet betalingstjenestedirektiv. Det retsgrundlag, der finder anvendelse i dette tilfælde, er derfor artikel 6, stk. 1, litra c), i databeskyttelsesforordningen.

28. Da databeskyttelsesforordningen har præciseret, at behandling på grundlag af en retlig forpligtelse bør være klart fastlagt i EU-retten eller en medlemsstats lovgivning (jf. artikel 6, stk. 3, i databeskyttelsesforordningen), bør forpligtelsen for kontoførende betalingstjenesteudbydere til at give adgang følge af den nationale lovgivning, der gennemfører det andet betalingstjenestedirektiv.

3 UDTRYKKELIGT SAMTYKKE

3.1 Samtykke i henhold til GDPR

29. I henhold til databeskyttelsesforordningen fungerer samtykke som et af de seks retsgrundlag for lovlig behandling af personoplysninger. I artikel 4, stk. 11, i databeskyttelsesforordningen defineres samtykke som "enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling". Disse fire betingelser, som er frivillige, specifikke, informerede og utvetydige, er afgørende for gyldigheden af samtykket. I henhold til Databeskyttelsesrådets retningslinjer 05/2020 om samtykke i henhold til forordning 2016/679 kan samtykke kun være et passende retsgrundlag, hvis en registreret tilbydes kontrol og et reelt valg med hensyn til at acceptere eller afvise de tilbudte vilkår eller afvise dem uden skadelige følger. Når en dataansvarlig anmoder om samtykke, er den dataansvarlige forpligtet til at vurdere, hvorvidt den dataansvarlige vil opfylde alle kravene i forbindelse med indhentning af gyldigt samtykke. Såfremt samtykket indhentes i fuld overensstemmelse med databeskyttelsesforordningen, er det et værktøj, der giver registrerede kontrol over, hvorvidt deres personoplysninger vil blive behandlet eller ej. Ellers er den registreredes kontrol illusorisk, og samtykket er et ugyldigt retsgrundlag for behandling, hvilket gør selve behandlingen ulovlig[21].

30. Databeskyttelsesforordningen indeholder også yderligere garantier i artikel 7, som fastsætter, at den dataansvarlige skal være i stand til at påvise, at der var gyldigt samtykke på behandlingstidspunktet. Desuden skal anmodningen om samtykke indgives på en måde, der klart kan skelnes fra de øvrige elementer, i en letforståelig og lettilgængelig form og i et klart og forståeligt sprog. Den registrerede skal ydermere oplyses om retten til at trække sit samtykke tilbage på et hvilket som helst tidspunkt på lige så enkel en måde, som det var at give samtykke.

31. I henhold til artikel 9 i databeskyttelsesforordningen er samtykke en af undtagelserne fra det generelle forbud mod behandling af særlige kategorier af personoplysninger. I så fald skal den registreredes samtykke dog være "udtrykkeligt"[22].

32. I henhold til Databeskyttelsesrådets retningslinjer 05/2020 om samtykke i henhold til forordning 2016/679 henviser udtrykkeligt samtykke i henhold til databeskyttelsesforordningen til den måde, hvorpå den registrerede giver samtykke. Det betyder, at den registrerede skal afgive en udtrykkelig erklæring om samtykke til et eller flere specifikke formål med behandlingen. Det ville være logisk at sikre, at samtykket er udtrykkeligt ved at bekræfte det i form af en skriftlig erklæring. Når det er hensigtsmæssigt, kan den dataansvarlige sørge for, at den skriftlige erklæring bliver underskrevet af den registrerede, så der fremadrettet ikke hersker nogen tvivl om og ikke er nogen risiko for, at der ikke foreligger noget bevis.

33. Samtykke kan under ingen omstændigheder udledes af potentielt tvetydige udsagn eller handlinger. Den dataansvarlige skal også være opmærksom på, at samtykke ikke kan opnås ved den handling, hvorved den registrerede undertegner en kontrakt eller accepterer almindelige betingelser og vilkår for en tjenesteydelse.

3.2 Samtykke i henhold til det andet betalingstjenestedirektiv

[21] Retningslinjer 05/2020 om samtykke i henhold til forordning 2016/679, Databeskyttelsesrådet, punkt 3.
[22] Se også udtalelse 15/2011 om definitionen af samtykke (WP 187), s. 6-8, og/eller udtalelse 06/2014 om den dataansvarliges legitime interesser i henhold til artikel 7 i direktiv 95/46/EF (WP 217), s. 9, 10, 13 og 14.

34. Databeskyttelsesrådet bemærker, at den retlige ramme for udtrykkeligt samtykke er kompleks, eftersom både det andet betalingstjenestedirektiv og databeskyttelsesforordningen omfatter begrebet "udtrykkeligt samtykke". Dette fører til spørgsmålet om, hvorvidt "udtrykkeligt samtykke" som nævnt i artikel 94, stk. 2, i det andet betalingstjenestedirektiv skal fortolkes på samme måde som udtrykkeligt samtykke i henhold til databeskyttelsesforordningen.

3.2.1 Udtrykkeligt samtykke i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv

35. Det andet betalingstjenestedirektiv indeholder en række specifikke regler vedrørende behandling af personoplysninger, navnlig artikel 94, stk. 1, i det andet betalingstjenestedirektiv, som fastsætter, at behandlingen af personoplysninger med henblik på det andet betalingstjenestedirektiv skal være i overensstemmelse med EU's databeskyttelseslovgivning. Endvidere fastsættes det i artikel 94, stk. 2, i det andet betalingstjenestedirektiv, at betalingstjenesteudbydere kun må tilgå, behandle og opbevare personoplysninger, der er nødvendige for leveringen af deres betalingstjenester, med betalingstjenestebrugerens udtrykkelige samtykke. I henhold til artikel 33, stk. 2, i det andet betalingstjenestedirektiv finder dette krav om betalingstjenestebrugerens udtrykkelige samtykke ikke anvendelse på kontooplysningstjenesteudbydere. Artikel 67, stk. 2, litra a), i det andet betalingstjenestedirektiv indeholder imidlertid stadig bestemmelser om udtrykkeligt samtykke for kontooplysningstjenesteudbydere vedrørende levering af tjenesten.

36. Som nævnt ovenfor er listen over retsgrundlag for behandling i henhold til betalingstjenestebrugeren udtømmende. Som nævnt i stk. 14 er retsgrundlaget for behandling af personoplysninger med henblik på levering af betalingstjenester i princippet artikel 6, stk. 1, litra b), i databeskyttelsesforordningen, hvilket betyder, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, eller for at træffe foranstaltninger på den registreredes anmodning forud for indgåelsen af en kontrakt. Det følger heraf, at artikel 94, stk. 2, i det andet betalingstjenestedirektiv ikke kan anses for et supplerende retsgrundlag for behandling af personoplysninger. I lyset af ovenstående mener Databeskyttelsesrådet, at dette stykke på den ene side bør fortolkes i overensstemmelse med den gældende retlige ramme for databeskyttelse, og på den anden side på en måde, der bevarer stykkets effektive virkning. Udtrykkeligt samtykke i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv bør derfor betragtes som et yderligere krav af kontraktmæssig karakter[23] i forbindelse med adgang til og efterfølgende behandling og lagring af personoplysninger med henblik på at udbyde betalingstjenester og er derfor ikke det samme som (udtrykkeligt) samtykke i henhold til databeskyttelsesforordningen.

37. "Udtrykkeligt samtykke" som omhandlet i artikel 94, stk. 2, i det andet betalingstjenestedirektiv er et kontraktligt samtykke. Dette indebærer, at artikel 94, stk. 2, i det andet betalingstjenestedirektiv bør fortolkes således, at de registrerede, når de indgår en aftale med en betalingstjenesteudbyder i henhold til det andet betalingstjenestedirektiv, skal gøres fuldt bekendt med de specifikke kategorier af personoplysninger, der vil blive behandlet. Desuden skal de gøres opmærksom på det specifikke (betalingstjenesterelaterede) formål, hvortil deres personoplysninger vil blive behandlet, og de skal udtrykkeligt acceptere disse bestemmelser. Sådanne bestemmelser bør klart kunne skelnes fra de øvrige elementer, der behandles i kontrakten, og de skal udtrykkeligt accepteres af den registrerede.

[23] Brev fra Databeskyttelsesrådet vedrørende det andet betalingstjenestedirektiv af 5. juli 2018, s. 4.

38. Kernen i begrebet "udtrykkeligt samtykke" i artikel 94, stk. 2, i det andet betalingstjenestedirektiv er at få adgang til personoplysninger for efterfølgende at behandle og lagre disse oplysninger med henblik at udbyde betalingstjenester. Dette lader forstå, at betalingstjenesteudbyderen[24] endnu ikke behandler personoplysningerne, men har brug for adgang til personoplysninger, der er blevet behandlet under en anden dataansvarligs ansvar. Hvis en betalingstjenestebruger indgår en aftale med f.eks. en betalingsinitieringstjenesteudbyder, skal denne udbyder have adgang til personoplysninger om betalingstjenestebrugeren, som behandles under den kontoførende betalingstjenesteudbyders ansvar. Formålet med det udtrykkelige samtykke i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv er at få tilladelse til at få adgang til disse personoplysninger for at kunne behandle og opbevare de personoplysninger, der er nødvendige for at udbyde betalingstjenesten. Hvis den registrerede giver udtrykkeligt samtykke, er den kontoførende betalingstjenesteudbyder forpligtet til at give adgang til de angivne personoplysninger.

39. Selv om samtykket i artikel 94, stk. 2, i det andet betalingstjenestedirektiv ikke er et retligt grundlag for behandling af personoplysninger, vedrører dette samtykke specifikt personoplysninger og databeskyttelse og sikrer gennemsigtighed og en vis grad af kontrol for betalingstjenestebrugeren[25]. Selv om det andet betalingstjenestedirektiv ikke præciserer de materielle betingelser for samtykke i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv, skal det, som anført ovenfor, forstås i overensstemmelse med den gældende retlige ramme for databeskyttelse og på en måde, der bevarer direktivets effektive virkning.

40. Med hensyn til de oplysninger, som de dataansvarlige skal give, og kravet om gennemsigtighed præciseres det i Artikel 29-Gruppens retningslinjer for gennemsigtighed, at "*en central overvejelse i forbindelse med gennemsigtighedsprincippet, som er beskrevet i disse bestemmelser, er, at den registrerede på forhånd bør kunne afgøre, hvad omfanget og konsekvenserne af behandlingen indebærer, og at de ikke på et senere tidspunkt bør blive overraskede over, hvordan deres personoplysninger er blevet brugt.*"[26].

41. Som krævet i princippet om formålsbegrænsning skal personoplysninger desuden indsamles til udtrykkeligt angivne og legitime formål (artikel 5, stk. 1, litra b), i databeskyttelsesforordningen). Hvis personoplysninger indsamles med mere end ét formål for øje, bør "*de dataansvarlige undgå kun at identificere ét bredt formål for at begrunde forskellige yderligere behandlingsaktiviteter, som faktisk kun er fjernt forbundet med det faktiske oprindelige formål*"[27]. Databeskyttelsesrådet har senest i forbindelse med kontrakter om onlinetjenester fremhævet risikoen for at medtage generelle behandlingsvilkår i kontrakter og har anført, at formålet med indsamlingen bør identificeres klart og specifikt: Denne identificering bør være tilstrækkeligt detaljeret til at afgøre, hvilken type behandling der er og ikke er omfattet af det angivne formål, og til at gøre det muligt at vurdere overholdelsen af lovgivningen og anvende databeskyttelsesgarantier[28].

[24] Dette gælder for tjenesteydelserne 1-7 i bilag 1 til det andet betalingstjenestedirektiv.
[25] Artikel 94, stk. 2, i det andet betalingstjenestedirektiv falder ind under kapitel 4 "Databeskyttelse".
[26] Artikel 29-Gruppens retningslinjer for gennemsigtighed i henhold til forordning 2016/679, punkt 10 (vedtaget den 11. april 2018) — godkendt af Databeskyttelsesrådet.
[27] Artikel 29-Gruppens udtalelse 03/2013 om formålsbegrænsning (WP203), s. 16.
[28] Retningslinje 2/2019 om behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i databeskyttelsesforordningen i forbindelse med levering af onlinetjenester til registrerede, punkt 16 (version fra offentlig høring) og artikel 29-Gruppens udtalelse 03/2013 om formålsbegrænsning (WP203), s. 15-16.

42. Når dette overvejes i forbindelse med det yderligere krav om udtrykkeligt samtykke i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv, indebærer dette, at dataansvarlige skal give de registrerede specifikke og udtrykkelige oplysninger om de specifikke formål, den dataansvarlige har identificeret som de formål, hvortil deres personoplysninger tilgås, behandles og opbevares. I overensstemmelse med artikel 94, stk. 2, i det andet betalingstjenestedirektiv skal de registrerede udtrykkeligt acceptere disse specifikke formål.

43. Som anført ovenfor i punkt 10 fremhæver Databeskyttelsesrådet desuden, at betalingstjenestebrugeren skal kunne vælge, om han eller hun vil benytte tjenesten eller ej, og ikke kan tvinges til at gøre det. Derfor skal samtykket i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv også være et frivilligt samtykke.

3.3 Konklusion

44. Udtrykkeligt samtykke i henhold til det andet betalingstjenestedirektiv adskiller sig fra (udtrykkeligt) samtykke i henhold til databeskyttelsesforordningen. Udtrykkeligt samtykke i henhold til artikel 94, stk. 2, i det andet betalingstjenestedirektiv er et yderligere krav af kontraktmæssig karakter. Når en betalingstjenesteudbyder har brug for adgang til personoplysninger for at kunne udbyde en betalingstjeneste, kræves der udtrykkeligt samtykke fra betalingstjenestebrugeren i overensstemmelse med artikel 94, stk. 2, i det andet betalingstjenestedirektiv.

4 BEHANDLING AF DATA FRA PASSIVE INTERESSENTER

4.1 Data fra passive interessenter

45. Et databeskyttelsesspørgsmål, der kræver nøje overvejelse, er behandlingen af såkaldte "data fra passive interessenter". I forbindelse med dette dokument er data fra passive interessenter personoplysninger om en registreret person, som ikke er bruger af en bestemt betalingstjenesteudbyder, men hvis personoplysninger behandles af den pågældende betalingstjenesteudbyder med henblik på opfyldelse af en kontrakt mellem udbyderen og betalingstjenestebrugeren. Dette er f.eks. tilfældet, når en betalingstjenestebruger, den registrerede A, gør brug af en kontooplysningstjenesteudbyders tjenester, og den registrerede B har foretaget en række betalingstransaktioner på den registrerede A's betalingskonto. I dette tilfælde betragtes den registrerede B som den "passive interessent", og personoplysningerne (såsom den registrerede B's kontonummer og det pengebeløb, der var involveret i disse transaktioner) vedrørende den registrerede B betragtes som "data fra passive interessenter".

4.2 Den dataansvarliges legitime interesse

46. Artikel 5, stk. 1, litra b), i databeskyttelsesforordningen kræver, at personoplysninger kun indsamles til udtrykkeligt angivne og legitime formål, og at de ikke må viderebehandles på en måde, der er uforenelig med disse formål. Desuden kræver databeskyttelsesforordningen, at enhver behandling af personoplysninger skal være både nødvendig og forholdsmæssig og i overensstemmelse med databeskyttelsesprincipperne, såsom principperne om formålsbegrænsning og dataminimering.

47. Databeskyttelsesforordningen kan give mulighed for behandling af data fra passive interessenter, når denne behandling er nødvendig for, at en dataansvarlig eller en tredjepart kan forfølge legitime interesser (artikel 6, stk. 1, litra f), i databeskyttelsesforordningen). En sådan behandling kan dog kun finde sted, når den dataansvarliges legitime interesse ikke "tilsidesættes af den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, som kræver beskyttelse af personoplysninger".

48. Et retsgrundlag for betalingsinitieringstjenesteudbyderes og kontooplysningstjenesteudbyderes behandling af data fra passive interessenter i forbindelse med levering af betalingstjenester i henhold til det andet betalingstjenestedirektiv kan således være en dataansvarligs eller tredjeparts legitime interesse i at opfylde kontrakten med betalingstjenestebrugeren. Nødvendigheden af at behandle den passive interessents personoplysninger er begrænset og afhænger af disse registreredes rimelige forventninger. I forbindelse med udbud af betalingstjenester, der er omfattet af det andet betalingstjenestedirektiv, skal der træffes effektive og passende foranstaltninger for at sikre, at de passive interessenters interesser eller grundlæggende rettigheder og frihedsrettigheder ikke tilsidesættes, og for at sikre, at disse registreredes rimelige forventninger til behandlingen af deres personoplysninger respekteres. I denne forbindelse skal den dataansvarlige (kontooplysningstjenesteudbyderen eller betalingsinitieringstjenesteudbyderen) tilvejebringe de nødvendige garantier for behandlingen for at beskytte de registreredes rettigheder. Dette omfatter tekniske foranstaltninger til at sikre, at data fra passive interessenter ikke behandles til et andet formål end det formål, hvortil personoplysningerne oprindeligt blev indsamlet af betalingsinitieringstjenesteudbydere og kontooplysningstjenesteudbydere. Hvis det er muligt, bør der også anvendes kryptering eller andre teknikker for at opnå et passende sikkerheds- og dataminimeringsniveau.

4.3 Yderligere behandling af personoplysninger om den passive interessent

49. Som anført i stk. 29 kan personoplysninger, der behandles i forbindelse med en betalingstjeneste, der er omfattet af det andet betalingstjenestedirektiv, behandles yderligere på grundlag af retlige forpligtelser, der påhviler tjenesteudbyderen. Disse retlige forpligtelser kan vedrøre personoplysninger om den passive interessent.

50. Med hensyn til yderligere behandling af data fra passive interessenter på grundlag af legitime interesser er Databeskyttelsesrådet af den opfattelse, at disse oplysninger ikke må anvendes til andre formål end dem, hvortil personoplysningerne er indsamlet, medmindre dette sker på grundlag af EU-retten eller medlemsstaternes nationale lovgivning. Det er ikke juridisk muligt at indhente samtykke fra den passive interessent, fordi det for at indhente samtykke vil være nødvendigt at indsamle eller behandle personoplysninger om den passive interessent, for hvilket der ikke kan findes noget retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen. Forenelighedstesten i databeskyttelsesforordningens artikel 6, stk. 4, kan heller ikke danne grundlag for behandlingen til andre formål (f.eks. direkte markedsføringsaktiviteter). Disse passive interessenters rettigheder og frihedsrettigheder vil ikke blive respekteret, hvis den nye dataansvarlige anvender personoplysningerne til andre formål, idet der tages hensyn til den sammenhæng, hvori personoplysningerne er indsamlet, navnlig fordi der ikke foreligger noget forhold til de registrerede, der er passive interessenter[29], fordi der ikke er nogen forbindelse mellem et andet formål og det formål, som personoplysningerne oprindeligt blev indsamlet til (dvs. det forhold, at betalingstjenesteudbydere kun har brug for data fra passive interessenter for at kunne opfylde en kontrakt med den anden kontraherende part) og grundet arten af de pågældende personoplysninger[30], den omstændighed, at de registrerede ikke med rimelighed kan forvente yderligere behandling eller endog være klar over, hvilken dataansvarlig der kan behandle deres personoplysninger, og i betragtning af de retlige begrænsninger for behandling, der er fastsat i artikel 66, stk. 3, litra g), og artikel 67, stk. 2, litra f), i det andet betalingstjenestedirektiv.

[29] Det fremgår af betragtning 87 i det andet betalingstjenestedirektiv, at det andet betalingstjenestedirektiv kun vedrører "aftalemæssige forpligtelser og ansvar mellem betalingstjenestebrugeren og betalingstjenesteudbyderen". Data fra passive interessenter falder derfor ikke ind under anvendelsesområdet for det andet betalingstjenestedirektiv.

[30] Der bør udvises særlig omhu ved behandling af finansielle personoplysninger, da behandlingen kan anses for at øge den mulige risiko for fysiske personers rettigheder og frihedsrettigheder i henhold til retningslinjerne for konsekvensanalyse vedrørende databeskyttelse.

5 BEHANDLING AF SÆRLIGE KATEGORIER AF PERSONOPLYSNINGER I HENHOLD TIL DET ANDET BETALINGSTJENESTEDIREKTIV

5.1 Særlige kategorier af personoplysninger

51. Artikel 9, stk. 1, i databeskyttelsesforordningen forbyder behandling af "personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering".

52. Det skal understreges, at elektroniske betalinger i nogle medlemsstater allerede er allestedsnærværende og foretrækkes af mange frem for kontanter i deres daglige transaktioner. Samtidig kan finansielle transaktioner afsløre følsomme oplysninger om en registreret, herunder oplysninger, der vedrører særlige kategorier af personoplysninger. Alt efter transaktionen kan politiske holdninger og religiøse overbevisninger f.eks. afsløres i forbindelse med bidrag til politiske partier eller organisationer, kirker eller sogne. Medlemskab af en fagforening kan afsløres ved, at der trækkes et årligt medlemskontingent fra en persons bankkonto. Personoplysninger om helbredsforhold kan indsamles ved at analysere lægeregninger, der betales af en registreret til en læge (f.eks. en psykiater). Endelig kan oplysninger om visse køb afsløre oplysninger om en persons seksuelle forhold eller seksuelle orientering. Som det fremgår af disse eksempler, kan selv enkelttransaktioner indeholde særlige kategorier af personoplysninger. Desuden kan kontooplysningstjenester benytte sig af profilering som defineret i artikel 4, stk. 4, i databeskyttelsesforordningen. Som tidligere anført i artikel 29-Gruppens retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, som godkendt af Databeskyttelsesrådet, kan der ved profilering "oprettes særlige kategorier af oplysninger ved at udlede fra oplysninger, der ikke er særlige kategorier af oplysninger i sig selv, men bliver det, når de kombineres med andre oplysninger"[31]. Dette betyder, at der gennem summen af finansielle transaktioner kan afsløres forskellige former for adfærdsmønstre, som kan omfatte særlige kategorier af personoplysninger. Der er derfor betydelig sandsynlighed for, at en tjenesteyder, der behandler oplysninger om registreredes finansielle transaktioner, også behandler særlige kategorier af personoplysninger.

53. Med hensyn til udtrykket "følsomme betalingsdata" bemærker Databeskyttelsesrådet følgende: Definitionen af følsomme betalingsdata i det andet betalingstjenestedirektiv afviger betydeligt fra den måde, hvorpå begrebet "følsomme personoplysninger" almindeligvis anvendes i forbindelse med databeskyttelsesforordningen og databeskyttelse (lovgivning). Hvor det andet betalingstjenestedirektiv definerer "følsomme betalingsdata" som "data, herunder personlige sikkerhedsoplysninger, som kan anvendes til at begå svig", understreger databeskyttelsesforordningen behovet for specifik beskyttelse af særlige kategorier af personoplysninger, som i henhold til artikel 9 i databeskyttelsesforordningen i sagens natur er særligt følsomme i forhold til grundlæggende rettigheder og frihedsrettigheder, såsom særlige kategorier af personoplysninger[32]. I den forbindelse anbefales det som minimum at kortlægge og kategorisere, præcist hvilken type personoplysninger der vil blive behandlet. Der vil sandsynligvis

[31] Artikel 29-Gruppen vedrørende Databeskyttelse, retningslinjer om automatiske individuelle afgørelser og profilering
i henhold til forordning 2016/679, WP251rev.01, s. 15.

[32] F.eks. betegnes særlige kategorier af personoplysninger i betragtning 10 i databeskyttelsesforordningen som "følsomme oplysninger".

være behov for en konsekvensanalyse vedrørende databeskyttelse i overensstemmelse med artikel 35 i databeskyttelsesforordningen, som vil bidrage til denne kortlægning. Der findes mere vejledning om konsekvensanalyser vedrørende databeskyttelse i artikel 29-Gruppens retningslinjer om konsekvensanalyse vedrørende databeskyttelse og fastlæggelse af, om behandling "sandsynligvis vil medføre en høj risiko" med henblik på forordning 2016/679, som godkendt af Databeskyttelsesrådet.

5.2 Mulige undtagelser

54. Forbuddet i artikel 9 i databeskyttelsesforordningen er ikke absolut. Der henvises navnlig til, at selv om undtagelser fra artikel 9, stk. 2, litra b) til f), og litra h) til j), i databeskyttelsesforordningen tydeligvis ikke finder anvendelse på behandling af personoplysninger inden for rammerne af det andet betalingstjenestedirektiv, kan følgende to undtagelser i artikel 9, stk. 2, i databeskyttelsesforordningen overvejes:

a) Forbuddet gælder ikke, hvis den registrerede har givet udtrykkeligt samtykke til behandling af disse personoplysninger til et eller flere specifikke formål (artikel 9, stk. 2, litra a), i databeskyttelsesforordningen).

b) Forbuddet gælder ikke, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale lovgivning, som skal stå i et rimeligt forhold til det tilstræbte mål, respektere kernen i retten til databeskyttelse og fastsætte passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser (artikel 9, stk. 2, litra g), i databeskyttelsesforordningen).

55. Det skal påpeges, at listen over undtagelser i artikel 9, stk. 2, i databeskyttelsesforordningen er udtømmende. Muligheden for, at der er inkluderet særlige kategorier af personoplysninger i de personoplysninger, der behandles med henblik på levering af de tjenester, som er omfattet af det andet betalingstjenestedirektiv, skal anerkendes af tjenesteudbyderen. Da forbuddet i artikel 9, stk. 1, i databeskyttelsesforordningen finder anvendelse på disse tjenesteudbydere, skal de sikre, at en af undtagelserne i artikel 9, stk. 2, i databeskyttelsesforordningen finder anvendelse på dem. Det skal understreges, at hvis tjenesteudbyderen ikke kan godtgøre, at en af undtagelserne er opfyldt, finder forbuddet i artikel 9, stk. 1, anvendelse.

5.3 Væsentlige samfundsinteresser

56. Betalingstjenester kan behandle særlige kategorier af personoplysninger af hensyn til væsentlige samfundsinteresser, men kun når alle betingelserne i artikel 9, stk. 2, litra g), i databeskyttelsesforordningen er opfyldt. Det betyder, at behandlingen af de særlige kategorier af personoplysninger skal behandles i en specifik undtagelse fra artikel 9, stk. 1, i databeskyttelsesforordningen i EU-retten eller medlemsstaternes nationale lovgivning. Denne bestemmelse skal omhandle proportionaliteten i forhold til det tilstræbte formål med behandlingen og indeholde passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Desuden skal denne bestemmelse i EU-retten eller medlemsstaternes nationale lovgivning respektere kernen i retten til databeskyttelse. Endelig skal det også påvises, at behandlingen af de særlige kategorier af oplysninger er nødvendig af hensyn til den væsentlige samfundsinteresse, herunder interesser af systemisk betydning. Kun når alle disse betingelser er opfyldt fuldt ud, kan denne undtagelse finde anvendelse på bestemte typer betalingstjenester.

5.4 Udtrykkeligt samtykke

57. I tilfælde, hvor undtagelsen i artikel 9, stk. 2, litra g), i databeskyttelsesforordningen ikke finder anvendelse, synes opnåelse af udtrykkeligt samtykke i overensstemmelse med betingelserne for gyldigt samtykke i databeskyttelsesforordningen fortsat at være den eneste mulige lovlige undtagelse for tredjepartsudbyderes behandling af særlige kategorier af personoplysninger. I Databeskyttelsesrådets retningslinjer 05/2020 om samtykke i henhold til forordning 2016/679 hedder det[33]: "Artikel 9, stk. 2, anerkender ikke "nødvendig for opfyldelse af en kontrakt" som en undtagelse fra det generelle forbud mod at behandle særlige kategorier af oplysninger. Derfor bør dataansvarlige og medlemsstater, der oplever denne situation, undersøge de specifikke undtagelser i artikel 9, stk. 2, litra b) til j). Når tjenesteudbydere påberåber sig artikel 9, stk. 2, litra a), i databeskyttelsesforordningen, skal de sikre, at de har fået udtrykkeligt samtykke, inden de påbegynder behandlingen." Udtrykkeligt samtykke som fastsat i artikel 9, stk. 2, litra a), i databeskyttelsesforordningen skal opfylde alle kravene i databeskyttelsesforordningen.

5.5 Ingen passende undtagelse

58. Som nævnt ovenfor finder forbuddet i artikel 9, stk. 1, anvendelse, når tjenesteyderen ikke kan påvise, at en af undtagelserne er opfyldt. I så tilfælde kan der træffes tekniske foranstaltninger for at forhindre behandling af særlige kategorier af personoplysninger, f.eks. ved at forhindre behandling af visse datapunkter. I den forbindelse kan betalingstjenesteudbydere undersøge de tekniske muligheder for at udelukke særlige kategorier af personoplysninger og tillade en selektiv adgang, hvilket ville forhindre tredjepartsudbydere i at behandle særlige kategorier af personoplysninger vedrørende passive interessenter.

[33] Retningslinjer 05/2020 om samtykke i henhold til forordning 2016/679, Databeskyttelsesrådet, punkt 99.

6 DATAMINIMERING, SIKKERHED, GENNEMSIGTIGHED, ANSVARLIGHED OG PROFILERING

6.1 Dataminimering og databeskyttelse gennem design og standardindstillinger

59. Princippet om dataminimering er nedfældet i artikel 5, stk. 1, litra c), i databeskyttelsesforordningen: "Personoplysninger skal være [...] tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles". Grundlæggende bør dataansvarlige i henhold til princippet om dataminimering ikke behandle flere personoplysninger, end hvad der er nødvendigt for at nå det pågældende specifikke formål. Som anført i kapitel 2 afhænger omfanget og arten af de personoplysninger, der er nødvendige for at levere betalingstjenesten, af det objektive og gensidigt forståede kontraktformål[34]. Dataminimering finder anvendelse på enhver behandling (f.eks. enhver indsamling af eller adgang til og anmodning om personoplysninger). Det fremgår af Databeskyttelsesrådets retningslinjer 4/2019 til artikel 25 om databeskyttelse gennem design og standardindstillinger, at "databehandlere og teknologiudbydere også anerkendes som centrale katalysatorer for databeskyttelse gennem design og standardindstillinger, og de bør også være opmærksomme på, at dataansvarlige kun må behandle personoplysninger ved hjælp af systemer og teknologier, der har indbygget databeskyttelse[35]" .

60. Artikel 25 i databeskyttelsesforordningen indeholder forpligtelser til at anvende databeskyttelse gennem design og standardindstillinger. Disse forpligtelser er af særlig betydning for princippet om dataminimering. I denne artikel fastsættes det, at dataansvarlige både på tidspunktet for fastlæggelsen af midlerne til behandling og på tidspunktet for selve behandlingen skal gennemføre passende tekniske og organisatoriske foranstaltninger, der er udformet med henblik på at gennemføre databeskyttelsesprincipperne på en effektiv måde og integrere de nødvendige garantier i behandlingen med henblik på at opfylde kravene i databeskyttelsesforordningen og beskytte registreredes rettigheder. Den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at der kun behandles personoplysninger, som er nødvendige til hvert specifikt formål med behandlingen. Denne forpligtelse gælder for den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Disse foranstaltninger kan omfatte kryptering, pseudonymisering og andre tekniske foranstaltninger.

61. Når forpligtelsen i artikel 25 i databeskyttelsesforordningen finder anvendelse, er de elementer, der skal tages hensyn til, det aktuelle tekniske niveau, gennemførelsesomkostningerne og arten og omfanget af og sammenhængen og formålene med behandlingen samt de risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen udgør. Der gives yderligere præciseringer om denne forpligtelse i Databeskyttelsesrådets ovennævnte retningslinjer 4/2019 til artikel 25 om databeskyttelse gennem design og standardindstillinger.

6.2 Dataminimeringsforanstaltninger

62. Den tredjepartsudbyder, der tilgår betalingskontodata for at kunne levere de ønskede tjenester, skal også tage hensyn til princippet om dataminimering og må kun indsamle personoplysninger,

[34] Retningslinjer 2/2019 om behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i databeskyttelsesforordningen i forbindelse med levering af onlinetjenester til registrerede, Databeskyttelsesrådet, stk. 32.
[35] Retningslinjer 4/2019 til artikel 25 om databeskyttelse gennem design og standardindstillinger, side 29.

der er nødvendige for at levere de specifikke betalingstjenester, som betalingstjenestebrugeren har anmodet om. Som princip bør adgangen til personoplysninger begrænses til, hvad der er nødvendigt for at udbyde betalingstjenester. Som det fremgår af kapitel 2, skal betalingstjenesteudbydere i henhold til det andet betalingstjenestedirektiv udveksle brugeroplysninger om betalingstjenester efter anmodning fra brugeren af betalingstjenester, når brugeren af betalingstjenesten ønsker at benytte en betalingsinitieringstjeneste eller en kontooplysningstjeneste.

63. Hvis det ikke er alle betalingskontodata, der er nødvendige for leveringen af kontrakten, skal kontooplysningstjenesteudbyderen udvælge de relevante datakategorier, inden dataene indsamles. F.eks. kan datakategorier, der muligvis ikke er nødvendige, omfatte identiteten af den passive interessent og transaktionens karakteristika. Medmindre det kræves i henhold til medlemsstatens eller EU's lovgivning, er det muligvis heller ikke nødvendigt at vise IBAN-nummeret på den passive interessents bankkonto.

64. I denne forbindelse kan der overvejes en eventuel anvendelse af tekniske foranstaltninger, der gør det muligt for eller støtter tredjepartsudbydere i deres forpligtelse til kun at tilgå og hente de personoplysninger, der er nødvendige for leveringen af deres tjenester, som led i gennemførelsen af passende databeskyttelsespolitikker i overensstemmelse med artikel 24, stk. 2, i databeskyttelsesforordningen. I den forbindelse anbefaler Databeskyttelsesrådet, at der anvendes digitale værktøjer til at støtte kontooplysningstjenesteudbyderne i deres forpligtelse til kun at indsamle personoplysninger, der er nødvendige til de formål, hvortil de behandles. Hvis en tjenesteudbyder f.eks. ikke har brug for transaktionskarakteristikaene (i beskrivelsesfeltet for transaktionsfortegnelserne) for at kunne levere sin tjeneste, kan et digitalt udvælgelsesværktøj fungere som et middel for tredjepartsudbydere til at udelukke dette felt fra tredjepartsudbyderens samlede behandlingsaktiviteter.

Eksempel 2:

HappyPayments, vores kontooplysningstjenesteudbyder fra eksempel 1, ønsker at sikre, at den kun behandler de personoplysninger om betalingskonti, som brugerne er interesseret i. Det vil ikke være nødvendigt at søge adgang til flere betalingskontodata for at kunne levere tjenesten. Den giver derfor brugerne mulighed for at vælge de specifikke typer oplysninger, de er interesseret i.

Bruger A ønsker en oversigt over sine udgifter i de sidste to måneder. Bruger A anmoder således om, for sine to bankkonti hos to forskellige kontoførende betalingstjenesteudbydere at få oplysninger om alle transaktioner i de sidste to måneder, transaktionsbeløbet, ekspeditionsdatoen og modtagerens navn, og markerer de tilsvarende felter i HappyPayments' brugergrænseflade.

HappyPayments anmoder herefter udelukkende de respektive kontoførende betalingstjenesteudbydere om de oplysninger, der svarer til de felter, bruger A markerede, og kun for de sidste to måneder. Der anmodes ikke om oplysninger såsom "informationsudveksling" i forbindelse med overførslen eller endda IBAN, da bruger A ikke bad om disse oplysninger.

For at gøre det muligt for HappyPayments at overholde sine dataminimeringsforpligtelser tillader de kontoførende betalingstjenesteudbydere HappyPayments at anmode om specifikke felter for en række datoer.

65. Det skal i denne forbindelse også bemærkes, at i henhold til det andet betalingstjenestedirektiv har kontoførende betalingstjenesteudbydere kun ret til at give adgang til oplysninger om betalingskonti. Der er ikke noget retsgrundlag i henhold til det andet betalingstjenestedirektiv for at give adgang til personoplysninger fra andre konti, såsom opsparingskonti, realkreditlåns- eller investeringskonti. I henhold til det andet betalingstjenestedirektiv skal der derfor gennemføres

tekniske foranstaltninger for at sikre, at adgangen begrænses til de nødvendige oplysninger om betalingskonti.

66. Ud over at indsamle så få data som muligt skal tjenesteudbyderen også indføre begrænsede opbevaringsperioder. Tjenesteudbyderen bør ikke opbevare personoplysninger længere, end hvad der er nødvendigt i forhold til de formål, som betalingstjenestebrugeren har anmodet om.

67. Hvis kontrakten mellem den registrerede og kontooplysningstjenesteudbyderen kræver videregivelse af personoplysninger til tredjeparter, må der kun videregives de personoplysninger, der er nødvendige for opfyldelsen af kontrakten. De registrerede bør også informeres specifikt om videregivelsen og de personoplysninger, der vil blive videregivet til denne tredjepart.

6.3 Sikkerhed

68. Databeskyttelsesrådet har allerede gjort opmærksom på, at krænkelse af finansielle personoplysninger *"tydeligvis indebærer alvorlige konsekvenser for den registreredes dagligdag*", og nævner risikoen for betalingssvig som eksempel[36].

69. Hvis et brud på datasikkerheden omfatter finansielle oplysninger, kan den registrerede være udsat for betydelige risici. Afhængigt af de oplysninger, der lækkes, kan de registrerede være udsat for en risiko for identitetstyveri, tyveri af midler på deres konti og andre aktiver. Desuden er der mulighed for, at eksponeringen af transaktionsdata er forbundet med betydelige risici for privatlivets fred, da transaktionsdata kan indeholde henvisninger til alle aspekter af den registreredes privatliv. Samtidig er finansielle data naturligvis værdifulde for kriminelle og derfor et attraktivt mål.

70. Som dataansvarlige er betalingstjenesteudbydere forpligtet til at træffe passende foranstaltninger til at beskytte registreredes personoplysninger (artikel 24, stk. 1, i databeskyttelsesforordningen). Jo højere risici, der er forbundet med den dataansvarliges behandlingsaktivitet, desto højere sikkerhedsstandarder skal der anvendes. Da behandlingen af finansielle data er forbundet med en række alvorlige risici, bør sikkerhedsforanstaltningerne være tilsvarende høje.

71. Tjenesteudbyderne bør leve op til høje standarder, herunder stærke kundeautentifikationsmekanismer og høje sikkerhedsstandarder for det tekniske udstyr[37]. Andre procedurer, såsom screening af databehandlere for sikkerhedsstandarder og gennemførelse af procedurer mod uautoriseret adgang, er også vigtige.

6.4 Gennemsigtighed og ansvarlighed

72. Gennemsigtighed og ansvarlighed er to grundlæggende principper i databeskyttelsesforordningen.

73. Med hensyn til gennemsigtighed (artikel 5, stk. 1, litra a), i databeskyttelsesforordningen) præciseres det i artikel 12 i databeskyttelsesforordningen, at dataansvarlige skal træffe passende foranstaltninger til at levere alle de oplysninger, der er omhandlet i artikel 13 og 14 i databeskyttelsesforordningen. Desuden kræves det, at oplysningerne eller kommunikationen om behandlingen af personoplysninger skal være kortfattede, gennemsigtige, forståelige og let tilgængelige. Oplysningerne skal være i et klart og forståeligt sprog og skriftlige "eller ad anden vej, herunder eventuelt ad elektronisk vej". Artikel 29-Gruppens retningslinjer for gennemsigtighed i

[36] Artikel 29-Gruppens retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis vil medføre en høj risiko" i henhold til forordning 2016/679, WP248 rev. 01 — godkendt af Databeskyttelsesrådet.
[37] Se de reguleringsmæssige tekniske standarder.

henhold til forordning 2016/679, som godkendt af Databeskyttelsesrådet, indeholder specifikke retningslinjer for overholdelse af princippet om gennemsigtighed i digitale miljøer.

74. I henhold til ovennævnte retningslinjer for gennemsigtighed i henhold til forordning 2016/679 bør artikel 11 i databeskyttelsesforordningen fortolkes som en måde til håndhævelse af reel dataminimering uden at hindre udøvelsen af registreredes rettigheder, og udøvelsen af registreredes rettigheder bør gøres mulig ved hjælp af yderligere oplysninger fra den registrerede. Der kan være situationer, hvor en dataansvarlig behandler personoplysninger, som ikke kræver identifikation af en registreret (f.eks. med pseudonymiserede oplysninger). I sådanne tilfælde kan artikel 11.1 også være relevant, da den fastsætter, at en dataansvarlig ikke er forpligtet til at opbevare, indhente eller behandle yderligere oplysninger for at identificere den registrerede alene med henblik på at overholde databeskyttelsesforordningen.

75. For tjenester i henhold til det andet betalingstjenestedirektiv finder artikel 13 i databeskyttelsesforordningen anvendelse på personoplysninger, der indsamles fra den registrerede, og artikel 14 finder anvendelse, hvis der ikke er indhentet personoplysninger fra den registrerede.

76. Den registrerede skal navnlig underrettes om det tidsrum, hvori personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til at fastsætte dette tidsrum, og, hvor det er relevant, de legitime interesser, der tilstræbes af den dataansvarlige eller en eventuel tredjepart. Hvis behandlingen er baseret på samtykke som omhandlet i artikel 6, stk. 1, litra a), i databeskyttelsesforordningen eller udtrykkeligt samtykke som omhandlet i artikel 9, stk. 2, litra a), i databeskyttelsesforordningen, skal den registrerede underrettes om retten til at trække sit samtykke tilbage til enhver tid.

77. Den dataansvarlige skal give oplysningerne til den registrerede under hensyntagen til de særlige omstændigheder, hvorunder personoplysningerne behandles. Hvis personoplysningerne skal anvendes til kommunikation med den registrerede[38], hvilket sandsynligvis vil være tilfældet for kontoførende betalingstjenesteudbydere, skal oplysningerne gives senest på tidspunktet for den første meddelelse til den registrerede. Hvis personoplysninger skal videregives til en anden modtager, skal oplysningerne gives, senest når personoplysningerne først videregives.

78. Med hensyn til onlinebetalingstjenester præciseres det i ovennævnte retningslinjer, at de dataansvarlige kan følge en lagdelt tilgang, hvis de vælger at anvende en kombination af metoder til at sikre gennemsigtighed. Det anbefales navnlig, at lagdelte databeskyttelseserklæringer/-meddelelser anvendes til at sammenkoble de forskellige kategorier af oplysninger, der skal gives til den registrerede, i stedet for at vise alle sådanne oplysninger i en enkelt meddelelse på en skærm, for at undgå informationstræthed og samtidig sikre oplysningernes virkningsfuldhed.

79. Ovennævnte retningslinjer præciserer også, at dataansvarlige kan vælge at anvende yderligere værktøjer til at give oplysninger til den enkelte registrerede, f.eks. databeskyttelsesdashboards. Et databeskyttelsesdashboard er et bestemt sted, hvor registrerede kan se "oplysninger om databeskyttelse" og administrere deres præferencer om beskyttelse af personoplysninger ved at tillade eller forhindre, at deres data anvendes på bestemte måder af den pågældende dataansvarlige[39]. Et databeskyttelsesdashboard kan give et overblik over de tredjepartsudbydere,

[38] Databeskyttelsesforordningen, artikel 14, stk. 3, litra b).

[39] I henhold til Artikel 29-Gruppens retningslinjer for gennemsigtighed i henhold til forordning 2016/679 — godkendt af Databeskyttelsesrådet er databeskyttelsesdashboards særligt nyttige, når den samme tjeneste

der har indhentet den registreredes udtrykkelige samtykke, og kan også give relevante oplysninger om arten og mængden af de personoplysninger, som tredjepartsudbydere har tilgået. I princippet kan en kontoførende betalingstjenesteudbyder give brugeren mulighed for at trække et specifikt udtrykkeligt samtykke i henhold til det andet betalingstjenestedirektiv[40] tilbage via oversigten, hvilket vil resultere i, at en eller flere tredjepartsudbydere nægtes adgang til den registreredes betalingskonti. Brugeren kan også anmode en kontoførende betalingstjenesteudbyder om at nægte en eller flere bestemte tredjepartsudbydere[41] adgang til sin(e) betalingskonto/-konti, da det er brugeren, der har ret til (ikke) at gøre brug af en kontooplysningstjeneste. Hvis der anvendes databeskyttelsesdashboards til at give eller trække et udtrykkeligt samtykke tilbage, bør de udformes og anvendes lovligt og navnlig forhindre, at der skabes hindringer for tredjepartsudbyderes ret til at levere tjenester i overensstemmelse med det andet betalingstjenestedirektiv. I denne henseende og i overensstemmelse med de gældende bestemmelser i det andet betalingstjenestedirektiv har en tredjepartsudbyder mulighed for at indhente udtrykkeligt samtykke fra brugeren igen, efter at dette samtykke er trukket tilbage.

80. Ansvarlighedsprincipperne kræver, at den dataansvarlige etablerer passende tekniske og organisatoriske foranstaltninger for at sikre og være i stand til at påvise, at behandlingen foretages i overensstemmelse med databeskyttelsesforordningen, navnlig med de vigtigste databeskyttelsesprincipper, der er fastsat i artikel 5, stk. 1. Disse foranstaltninger bør tage hensyn til behandlingens karakter, omfang, kontekst og formål samt til risikoen for fysiske personers rettigheder og frihedsrettigheder, og foranstaltningerne skal revideres og ajourføres, når det er nødvendigt[42].

6.5 Profilering

81. Betalingstjenesteudbyderes behandling af personoplysninger kan indebære "profilering" som omhandlet i artikel 4, stk. 4, i databeskyttelsesforordningen. Kontoførende betalingstjenesteudbydere kan f.eks. benytte sig af automatisk behandling af personoplysninger med henblik på at vurdere visse personlige aspekter vedrørende en fysisk person. En registrerets personlige økonomiske situation kan blive vurderet, afhængigt af tjenestens særlige karakteristika. Kontooplysningstjenester, der skal leveres på brugernes anmodning, kan omfatte en omfattende vurdering af personoplysninger om betalingskonti.

82. Den dataansvarlige skal også være åben over for den registrerede om eksistensen af automatiseret beslutningstagning, herunder profilering. I sådanne tilfælde skal den dataansvarlige give meningsfulde oplysninger om den involverede logik samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede (artikel 13, stk. 2, litra f), og artikel 14, stk. 2, litra g), og betragtning 60)[43]. På samme måde har den registrerede i henhold til artikel 15 i databeskyttelsesforordningen ret til at anmode om og indhente oplysninger fra den dataansvarlige

---

anvendes af registrerede på en række forskellige anordninger, da de giver dem adgang til og kontrol over deres personoplysninger, uanset hvordan de bruger tjenesten. Når de registrerede får mulighed for manuelt at justere deres privatlivsindstillinger via et databeskyttelsesdashboard, kan det også gøre det lettere at individualisere en erklæring/meddelelse om databeskyttelse, så den kun afspejler de behandlingstyper, der forekommer for den pågældende registrerede.

[40] Se f.eks. det "udtrykkelige samtykke", der er nævnt i artikel 67, stk. 2, litra a), i det andet betalingstjenestedirektiv.

[41] Se også EBA/OP/2020/10, punkt 45.

[42] Databeskyttelsesforordningen, artikel 5, stk. 2, og artikel 24.

[43] Retningslinjer for gennemsigtighed i henhold til forordning 2016/679, WP 260 rev. 01 — godkendt af Databeskyttelsesrådet.

om eksistensen af automatisk beslutningstagning, herunder profilering, den involverede logik og konsekvenserne for den registrerede, samt under visse omstændigheder ret til at gøre indsigelse mod profilering, uanset om der foretages rent automatisk individuel beslutningstagning baseret på profilering eller ej[44].

83. Det relevante i denne forbindelse er desuden også den registreredes ret til ikke at være genstand for en afgørelse, der udelukkende er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis påvirker den pågældende væsentligt, jf. artikel 22 i databeskyttelsesforordningen. Denne norm omfatter også under visse omstændigheder behovet for, at de dataansvarlige gennemfører passende foranstaltninger til beskyttelse af den registreredes rettigheder, såsom specifikke oplysninger til den registrerede, retten til menneskelig indgriben i beslutningstagningen og til at udtrykke sine synspunkter og anfægte afgørelsen. Som det også fremgår af betragtning 71 i databeskyttelsesforordningen, betyder dette bl.a., at registrerede har ret til ikke at blive genstand for en afgørelse såsom automatisk afvisning af en onlinekreditansøgning uden menneskelig indgriben[45].

84. Automatiseret beslutningstagning, herunder profilering, der omfatter særlige kategorier af personoplysninger, er kun tilladt på de kumulative betingelser i artikel 22, stk. 4, i databeskyttelsesforordningen:

- Der er en gældende undtagelse i henhold til artikel 22, stk. 2.
- Artikel 9, stk. 2, litra a) eller g), i databeskyttelsesforordningen finder anvendelse. I begge tilfælde skal den dataansvarlige træffe passende foranstaltninger til at beskytte den registreredes rettigheder, frihedsrettigheder og legitime interesser[46].

85. Kravene til viderebehandling som anført i disse retningslinjer bør også overholdes. Præciseringerne og instrukserne om automatiseret individuel beslutningstagning og profilering i Artikel 29-Gruppens retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, som godkendt af Databeskyttelsesrådet, er fuldt ud relevante i forbindelse med betalingstjenester og bør derfor tages behørigt i betragtning.

På vegne af Det Europæiske Databeskyttelsesråd

Formand

(Andrea Jelinek)

[44] Artikel 29-Gruppens retningslinjer for om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP251rev.01.
[45] Betragtning 71 i databeskyttelsesforordningen.
[46] Artikel 29-Gruppens retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP251rev.01., side 24.