

Orientări



**Orientările 06/2020 privind interacțiunea dintre A doua
directivă privind serviciile de plată și RGPD**

Versiunea 2.0

Adoptată la 15 decembrie 2020

Istoric versiuni

Versiunea 2.0	15.12.2020	Adoptarea orientărilor în urma consultării publice
Versiunea 1.0	17.7.2020	Adoptarea orientărilor spre consultare publică

Cuprins

1. Introducere.....	54
1.1 Definiții	64
1.2 Servicii în temeiul DSP2.....	74
2 Temeiurile legale și prelucrarea ulterioară în temeiul DSP2.....	104
2.1 Temeiuri legale pentru prelucrare	104
2.2 Articolul 6 alineatul (1) litera (b) din RGPD (prelucrarea este necesară pentru executarea unui contract).....	104
2.3 Prevenirea fraudelor	124
2.4 Prelucrare ulterioară (PSIC și PSIP).....	124
2.5 Temeiul legal pentru acordarea accesului la cont (PSPSAC).....	134
3 Consimțământul explicit.....	144
3.1 Consimțământ în temeiul RGPD.....	144
3.2 Consimțământ în temeiul DSP2.....	154
3.2.1 Consimțământ explicit în temeiul articolului 94 alineatul (2) din DSP2.....	154
3.3 Concluzie	174
4 Prelucrarea datelor părților pasive	184
4.1 Datele părților pasive	184
4.2 Interesul legitim al operatorului.....	184
4.3 Prelucrarea ulterioară a datelor cu caracter personal ale părții pasive.....	184
5 Prelucrarea categoriilor speciale de date cu caracter personal în temeiul DSP2	204
5.1 Categoriile speciale de date cu caracter personal	204
5.2 Derogări posibile	214
5.3 Interesul public major	214
5.4 Consimțământul explicit.....	224
5.5 Nicio derogare adecvată.....	224
6 Reducerea la minimum a datelor, securitatea, transparența, responsabilitatea și crearea de profiluri.....	234
6.1 Reducerea la minimum a datelor și protecția datelor începând cu momentul conceperii și în mod implicit.....	234
6.2 Măsuri de reducere la minimum a datelor	234
6.3 Securitate	254
6.4 Transparență și răspundere	254
6.5 Crearea de profiluri	274

Comitetul european pentru protecția datelor,

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018¹,

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

întrucât:

(1) Regulamentul general privind protecția datelor prevede un set coerent de norme pentru prelucrarea datelor cu caracter personal la nivelul întregii Uniuni.

(2) A doua directivă privind serviciile de plată [Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 23 decembrie 2015, denumită în continuare „DSP2”)] abrogă Directiva 2007/64/CE și prevede noi norme pentru a asigura securitatea juridică pentru consumatori, comercianți și întreprinderi în cadrul lanțului de plăți și pentru a moderniza cadrul juridic al pieței serviciilor de plată². Statele membre au avut obligația de a transpune DSP2 în dreptul intern până la 13 ianuarie 2018.

(3) O caracteristică importantă a DSP2 este introducerea unui cadru juridic pentru noi servicii de inițiere a plăților și servicii de informare cu privire la conturi. DSP2 permite acestor noi prestatori de servicii de plată să obțină acces la conturile de plăți ale persoanelor vizate în scopul furnizării serviciilor respective.

(4) În ceea ce privește protecția datelor, în conformitate cu articolul 94 alineatul (1) din DSP2, orice prelucrare a datelor cu caracter personal, inclusiv furnizarea de informații cu privire la prelucrare, în scopul DSP2, se efectuează în conformitate cu RGPD³ și cu Regulamentul (UE) 2018/1725.

(5) Considerentul 89 din DSP2 prevede că, în cazul în care datele cu caracter personal sunt prelucrate în sensul DSP2, ar trebui să se precizeze obiectivul precis al prelucrării, să se menționeze temeiul juridic aplicabil, să se pună în aplicare cerințele de securitate relevante prevăzute în RGPD, iar principiile necesității, proporționalității, limitării scopului și perioadei proporționale de reținere a datelor ar trebui să fie respectate. De asemenea, protecția datelor începând cu momentul conceperii și protecția implicită a datelor ar trebui să fie incluse în toate sistemele de prelucrare a datelor elaborate și utilizate în cadrul DSP2⁴.

(6) Considerentul 93 din DSP2 prevede că prestatorii de servicii de inițiere a plății și prestatorii de servicii de informare cu privire la conturi, pe de o parte, și, pe de altă parte, prestatorul de servicii de plată care oferă servicii de administrare cont ar trebui să respecte cerințele necesare privind protecția

¹ Trimiterile la „statele membre” din prezentul document trebuie înțelese ca trimiteri la „statele membre ale SEE”.

² Considerentul 6 din DSP2.

³ Întrucât DSP2 a fost adoptată înainte de RGPD, aceasta face în continuare trimitere la Directiva 95/46. Articolul 94 din RGPD prevede că trimiterile la Directiva 95/46/CE abrogată se interpretează ca trimiteri la RGPD.

⁴ Considerentul 89 din DSP2.

și securitatea datelor stabilite sau menționate în directiva menționată ori incluse în cadrul standardelor tehnice de reglementare,

ADOPTĂ URMĂTOARELE ORIENTĂRI

1. INTRODUCERE

1. A doua directivă privind serviciile de plată (denumită în continuare „DSP2”) a introdus o serie de noutăți în domeniul serviciilor de plată. Deși creează noi oportunități pentru consumatori și sporește transparența în acest domeniu, aplicarea DSP2 ridică anumite întrebări și preocupări cu privire la necesitatea ca persoanele vizate să păstreze controlul deplin asupra datelor lor cu caracter personal. Regulamentul general privind protecția datelor (denumit în continuare „RGPD”) se aplică prelucrării datelor cu caracter personal, inclusiv activităților de prelucrare efectuate în contextul serviciilor de plată, astfel cum sunt definite în DSP2⁵. Astfel, operatorii care acționează în domeniul reglementat de DSP2 trebuie să asigure întotdeauna conformitatea cu cerințele RGPD, inclusiv cu principiile privind protecția datelor, prevăzute la articolul 5 din RGPD, precum și cu dispozițiile relevante ale Directivei asupra confidențialității și comunicațiilor electronice⁶. Deși DSP2⁷ și standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise comune și sigure de comunicare (denumite în continuare „STR”⁸) conțin anumite dispoziții referitoare la protecția și securitatea datelor, au apărut incertitudini cu privire la interpretarea acestor dispoziții, precum și la interacțiunea dintre cadrul general de protecție a datelor și DSP2.
2. La 5 iulie 2018, CEPD a emis o scrisoare privind DSP2, în care a oferit clarificări cu privire la chestiuni referitoare la protecția datelor cu caracter personal în legătură cu DSP2, în special cu privire la prelucrarea datelor cu caracter personal ale părților necontractante (așa-numitele „date ale părților pasive”) de către prestatorii de servicii de informare cu privire la conturi (denumiți în continuare „PSIC”) și prestatorii de servicii de inițiere a plății (denumiți în continuare „PSIP”), procedurile referitoare la acordarea și retragerea consimțământului, STR și cooperarea dintre prestatorii de servicii de plată care oferă servicii de administrare cont (denumiți în continuare „PSPSAC”). Întrucât lucrările pregătitoare ale acestor orientări au implicat colectarea de contribuții de la părțile interesate, atât în scris, cât și în cadrul unui eveniment al părților interesate, pentru a identifica cele mai urgente provocări.
3. Scopul prezentelor orientări este de a oferi îndrumări suplimentare cu privire la aspectele legate de protecția datelor în contextul DSP2, în special cu privire la relația dintre dispozițiile relevante privind RGPD și DSP2. Prezentele orientări se axează în principal pe prelucrarea datelor cu caracter

⁵ Articolul 1 alineatul (1) din RGPD.

⁶ Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva ~~asupra confidențialității~~ privind viața privată și comunicațiile electronice); JO L 201, 31.7.2002, p. 0037-0047.

⁷ Articolul 94 din DSP etc.

⁸ Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare (Text cu relevanță pentru SEE.); C/2017/7782; JO L 69, 13.3.2018, p. 23-43; disponibil la <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018R0389&from=RO>.

personal de către PSIC și PSIP. Prin natura sa, prezentul document îndeplinește condițiile pentru acordarea accesului la informațiile privind conturile de plăți de către PPSAC și pentru prelucrarea datelor cu caracter personal de către PSIP și PSIC, inclusiv cerințele și garanțiile referitoare la prelucrarea datelor cu caracter personal de către PSIP și PSIC în alte scopuri decât scopurile inițiale pentru care au fost colectate datele, în special atunci când acestea au fost colectate în contextul furnizării unui serviciu de informare cu privire la conturi⁹. Prezentul document abordează, de asemenea, diferite noțiuni de consimțământ explicit în temeiul DSP2 și al RGPD, prelucrarea „datelor părților pasive”, prelucrarea categoriilor speciale de date cu caracter personal de către PSIP și PSIC, aplicarea principiilor fundamentale de protecție a datelor prevăzute de RGPD, inclusiv reducerea la minimum a datelor, transparența, responsabilitatea și măsurile de securitate. DSP2 implică responsabilități interfuncționale în domenii precum protecția consumatorilor și dreptul concurenței. Considerațiile privind aceste domenii juridice depășesc domeniul de aplicare al prezentelor orientări.

4. Pentru a facilita lectura orientărilor, mai jos sunt prezentate principalele definiții utilizate în prezentul document.

1.1 Definiții

„prestator de servicii de informare cu privire la conturi” („PSIC”) înseamnă un prestator de servicii online care furnizează informații consolidate în legătură cu unul sau mai multe conturi de plăți deținute de utilizatorul serviciilor de plată fie la un alt prestator de servicii de plată, fie la mai mulți prestatori de servicii de plată;

„prestator de servicii de plată care oferă servicii de administrare cont” („PPSAC”) înseamnă un prestator de servicii de plată care furnizează și administrează un cont de plăți pentru un plătitor;

„reducerea la minimum a datelor” înseamnă un principiu al protecției datelor, conform căruia datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;

„plătitor” înseamnă persoana fizică sau juridică care este titularul unui cont de plăți și care autorizează un ordin de plată din acel cont de plăți sau, în cazul în care nu este vorba de un cont de plăți, persoana fizică sau juridică care emite un ordin de plată;

„beneficiar al plății” înseamnă o persoană fizică sau juridică căreia îi sunt destinate fondurile care au făcut obiectul unei operațiuni de plată;

„cont de plăți” înseamnă un cont deținut în numele unuia sau al mai multor utilizatori de servicii de plată, care este folosit pentru executarea operațiunilor de plată;

„prestator de servicii de inițiere a plății” („PSIP”) înseamnă un prestator care desfășoară un serviciu de inițiere a unui ordin de plată la cererea utilizatorului serviciilor de plată cu privire la un cont de plăți deținut la un alt prestator de servicii de plată;

⁹ Un serviciu de informare cu privire la conturi înseamnă un serviciu online care furnizează informații consolidate în legătură cu unul sau mai multe conturi de plăți deținute de utilizatorul serviciilor de plată fie la un alt prestator de servicii de plată, fie la mai mulți prestatori de servicii de plată.

„prestator de servicii de plată” înseamnă o entitate menționată la articolul 1 alineatul (1) din DSP2¹⁰ sau o persoană fizică sau juridică care beneficiază de o derogare în temeiul articolului 32 sau 33 din DSP2;

„utilizator al serviciilor de plată” înseamnă persoana fizică sau juridică ce folosește un serviciu de plată în calitate de plătitor, de beneficiar al plății sau în ambele calități;

„date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

„protecția datelor începând cu momentul conceperii” înseamnă măsurile tehnice și organizatorice încorporate într-un produs sau serviciu, care sunt concepute pentru a pune în aplicare principiile de protecție a datelor într-un mod eficace și pentru a integra garanțiile necesare în prelucrare în vederea îndeplinirii cerințelor RGPD și a protejării drepturile persoanelor vizate;

„protecția datelor în mod implicit” înseamnă măsurile tehnice și organizatorice adecvate puse în aplicare într-un produs sau serviciu care asigură faptul că, în mod implicit, sunt prelucrate numai datele cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării;

„STR” înseamnă Regulamentul delegat (UE) 2018/389 al Comisiei din 27 noiembrie 2017 de completare a Directivei (UE) 2015/2366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare;

„prestatori terți” („PT”) înseamnă atât PSIP, cât și PSIC.

1.2 Servicii în temeiul DSP2

5. DSP2 introduce două noi tipuri de servicii de plată (prestatori): PSIP și PSIC. Anexa 1 la DSP2 conține cele opt servicii de plată care fac obiectul DSP2.

¹⁰ Articolul 1 alineatul (1) din DSP2 prevede că DSP2 stabilește normele conform cărora statele membre fac distincție între următoarele categorii de *prestatori de servicii de plată*:

(a) instituții de credit astfel cum sunt definite la articolul 4 alineatul (1) punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului (1), inclusiv sucursalele acestora, în sensul articolului 4 alineatul (1) punctul 17 din regulamentul respectiv în cazul în care astfel de sucursale sunt situate în Uniune, indiferent dacă sediile centrale ale sucursalelor respective sunt situate în Uniune, sau, în conformitate cu articolul 47 din Directiva 2013/36/UE și cu dreptul intern, sunt situate în afara Uniunii;

(b) instituții emitente de monedă electronică în sensul articolului 2 punctul 1 din Directiva 2009/110/CE inclusiv, în conformitate cu articolul 8 din respectiva directivă și cu dreptul intern, sucursalele acestora, în cazul în care astfel de sucursale sunt situate în Uniune, iar sediile centrale ale acestora sunt situate în afara Uniunii și, în măsura în care serviciile de plată prestate de respectivele sucursale sunt legate de emiterea de monedă electronică;

(c) oficii poștale care efectuează operațiuni de virament care sunt îndreptățite, în temeiul dreptului intern, să presteze servicii de plată;

(d) instituții de plată;

(e) BCE și băncile centrale naționale, atunci când nu acționează în calitate lor de autoritate monetară sau de alte autorități publice;

(f) statele membre sau autoritățile lor regionale sau locale, atunci când nu acționează în calitate lor de autorități publice.

6. PSIP furnizează servicii de inițiere a ordinelor de plată la cererea utilizatorului serviciilor de plată în legătură cu contul de plăți al utilizatorului deținut la un alt prestator de servicii de plată¹¹. Un PSIP poate solicita unui PSPSAC (de obicei, o bancă) să inițieze o operațiune în numele utilizatorului serviciilor de plată. Utilizatorul (serviciului de plată) poate fi o persoană fizică (persoană vizată) sau o persoană juridică.
7. PSIC oferă servicii online pentru informații consolidate în legătură cu unul sau mai multe conturi de plăți deținute de utilizatorul serviciilor de plată fie la un alt prestator de servicii de plată, fie la mai mulți prestatori de servicii de plată¹². Potrivit considerentului 28 din DSP2, utilizatorul serviciilor de plată poate avea imediat, în orice moment, o imagine de ansamblu asupra situației sale financiare.
8. În ceea ce privește serviciile de informare cu privire la conturi, ar putea exista mai multe tipuri diferite de servicii oferite, cu accent pe caracteristici și scopuri diferite. De exemplu, unii prestatori pot oferi utilizatorilor servicii precum planificarea bugetară și monitorizarea cheltuielilor. Prelucrarea datelor cu caracter personal în contextul acestor servicii este reglementată de DSP2. Serviciile care implică evaluări ale bonității utilizatorului serviciilor de plată sau serviciile de audit efectuate pe baza colectării de informații prin intermediul unui serviciu de informare cu privire la conturi nu se încadrează în domeniul de aplicare al DSP2 și, prin urmare, intră sub incidența RGPD. În plus, nici alte conturi decât conturile de plăți (de exemplu, economii, investiții) nu sunt acoperite de DSP2. În orice caz, RGPD este cadrul juridic aplicabil pentru prelucrarea datelor cu caracter personal.

Exemplul 1.

HappyPayments este o societate care oferă un serviciu online constând în furnizarea de informații privind unul sau mai multe conturi de plăți prin intermediul unei aplicații pentru dispozitive mobile pentru a asigura supravegherea financiară (un serviciu de informare cu privire la conturi). Prin intermediul acestui serviciu, utilizatorul serviciilor de plată poate vedea imediat soldurile și operațiunile recente în două sau mai multe conturi de plăți la bănci diferite. De asemenea, la alegerea unui utilizator al serviciilor de plată, aceasta oferă o clasificare a cheltuielilor și veniturilor în funcție de diferite tipologii (salariu, timp liber, energie, ipotecă etc.), ajutându-l astfel pe utilizatorul serviciilor de plată cu planificarea financiară. În această aplicație, HappyPayments oferă, de asemenea, un serviciu de inițiere a plăților direct din contul (conturile) de plăți desemnat(e) de utilizatori (un serviciu de inițiere a plăților).

9. Pentru a furniza aceste servicii, DSP2 reglementează condițiile legale în care PSIP și PSIC pot accesa conturi de plăți pentru a furniza un serviciu utilizatorului serviciilor de plată.
10. La articolul 66 alineatul (1) și la articolul 67 alineatul (1) din DSP2 se prevede că accesul la serviciile de plată și de informare cu privire la conturi și utilizarea acestora sunt drepturi ale utilizatorului serviciilor de plată. Aceasta înseamnă că utilizatorul serviciilor de plată ar trebui să aibă libertate deplină în ceea ce privește exercitarea acestui drept și nu poate fi obligat să facă uz de acest drept.
11. Accesul la conturile de plăți și utilizarea informațiilor privind conturile de plăți sunt parțial reglementate la articolele 66 și 67 din DSP2, care conțin garanții privind protecția datelor (cu caracter personal). Articolul 66 alineatul (3) litera (f) din DSP2 prevede că PSIP nu solicită din partea utilizatorului serviciilor de plată alte date decât cele necesare pentru prestarea serviciului

¹¹ Articolul 4 alineatul (15) din DSP2.

¹² Articolul 4 alineatul (16) din DSP2.

de inițiere a plății, iar articolul 66 alineatul (3) litera (g) din DSP2 prevede că PSIP nu utilizează, nu accesează și nu stochează niciun fel de date în alte scopuri decât pentru prestarea serviciului de inițiere a plății solicitat explicit de utilizatorul serviciilor de plată. În plus, articolul 67 alineatul (2) litera (d) din DSP2 limitează accesul PSIC la informațiile provenind de la conturi de plată desemnate și de la operațiunile de plată aferente, în timp ce articolul 67 alineatul (2) litera (f) din DSP2 prevede că PSIC nu utilizează, nu accesează sau nu stochează niciun fel de date în alte scopuri decât pentru prestarea serviciului de informare cu privire la conturi solicitat explicit de către utilizatorul serviciilor de plată, în conformitate cu normele de protecție a datelor. Acesta din urmă subliniază că, în cadrul serviciilor de informare cu privire la conturi, datele cu caracter personal pot fi colectate numai în scopuri determinate, explicite și legitime. Prin urmare, un PSIC ar trebui să precizeze în contract scopurile specifice pentru care urmează să fie prelucrate datele privind contul personal, în contextul serviciului de informare cu privire la conturi pe care îl prestează. Contractul ar trebui să fie legal, echitabil și transparent în temeiul articolului 5 din RGPD și să respecte, de asemenea, alte legi privind protecția consumatorilor.

12. În funcție de circumstanțe specifice, prestatorii de servicii de plată ar putea fi operatori sau persoane împuternicite de către operator în temeiul RGPD. În cadrul prezentelor orientări, „operatorii” sunt prestatorii de servicii de plată care, singuri sau împreună cu alții, stabilesc scopurile și mijloacele de prelucrare a datelor cu caracter personal. Îndrumări suplimentare în acest sens sunt disponibile în Orientările CEPD nr. 07/2020 privind conceptele de operator și de persoană împuternicită de către operator din RGPD.

2 TEMEIURILE LEGALE ȘI PRELUCRAREA ULTERIOARĂ ÎN TEMEIUL DSP2

2.1 Temeiuri legale pentru prelucrare

13. În temeiul RGPD, operatorii trebuie să aibă un temei juridic pentru prelucrarea datelor cu caracter personal. Articolul 6 alineatul (1) din RGPD constituie o listă exhaustivă și restrictivă de șase temeiuri juridice pentru prelucrarea datelor cu caracter personal în temeiul RGPD¹³. Este la latitudinea operatorului să definească temeiul juridic adecvat și să se asigure că sunt îndeplinite toate condițiile pentru acest temei juridic. Pentru a stabili care temei juridic se aplică și care este cel mai adecvat într-o situație specifică trebuie să se țină seama de circumstanțele în care se efectuează prelucrarea, inclusiv de scopul prelucrării și de relația dintre operator și persoana vizată.

2.2 Articolul 6 alineatul (1) litera (b) din RGPD (prelucrarea este necesară pentru executarea unui contract)

14. Serviciile de plată sunt prestate în baza unui contract încheiat între utilizatorul serviciilor de plată și prestatorul de servicii de plată. După cum se menționează la considerentul 87 din DSP2, „[p]rezenta directivă ar trebui să se refere doar la obligațiile și la responsabilitățile contractuale dintre utilizatorul serviciilor de plată și prestatorul de servicii de plată.” În sensul RGPD, principalul temei juridic pentru prelucrarea datelor cu caracter personal pentru prestarea de servicii de plată este articolul 6 alineatul (1) litera (b) din RGPD, ceea ce înseamnă că prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract.

15. Serviciile de plată în temeiul DSP2 sunt definite în anexa 1 la DSP2. Prestarea acestor servicii, astfel cum este definită în DSP2, este o cerință pentru încheierea unui contract în care părțile au acces la datele privind contul de plăți ale utilizatorului serviciilor de plată. Acești prestatori de servicii de plată trebuie să fie, de asemenea, operatori autorizați. În ceea ce privește serviciile de inițiere a plății și serviciile de informare cu privire la conturi în temeiul DSP2, contractele pot include clauze care impun, de asemenea, condiții privind serviciile suplimentare care nu sunt reglementate de

¹³ În conformitate cu articolul 6, prelucrarea datelor cu caracter personal este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

- (a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- (b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- (c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- (d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- (e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;
- (f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

DSP2. *Orientările CEPD 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate* clarifică faptul că operatorii trebuie să evalueze ce prelucrare a datelor cu caracter personal este obiectiv necesară pentru a executa contractul. Aceste orientări subliniază că justificarea necesității depinde de natura serviciului, de perspectivele și așteptările reciproce ale părților contractante, de motivul contractului și de elementele esențiale ale contractului.

16. Orientările CEPD 2/2019 clarifică, de asemenea, faptul că, având în vedere articolul 7 alineatul (4) din RGPD, se face o distincție între activitățile de prelucrare necesare pentru executarea unui contract și clauzele care condiționează serviciul de anumite activități de prelucrare care nu sunt efectiv necesare pentru executarea contractului. Sintagma „necesar pentru executare” impune în mod clar ceva mai mult decât o clauză contractuală¹⁴. Operatorul ar trebui să fie în măsură să demonstreze modul în care obiectul principal al contractului specific cu persoana vizată nu poate fi realizat, de fapt, dacă nu are loc prelucrarea specifică a datelor cu caracter personal în cauză. Simpla referință sau mențiune privind prelucrarea datelor într-un contract nu este suficientă pentru a considera că respectiva prelucrare a datelor intră sub incidența domeniului de aplicare al articolului 6 alineatul (1) litera (b) din RGPD.
17. Articolul 5 alineatul (1) litera (b) din RGPD prevede principiul limitărilor legate de scop, care impune ca datele cu caracter personal să fie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri. Atunci când se evaluează dacă articolul 6 alineatul (1) litera (b) reprezintă un temei juridic adecvat pentru un serviciu (de plată) online, ar trebui să se țină seama de intenția, scopul sau obiectivul specific al serviciului¹⁵. Scopurile prelucrării trebuie să fie specificate în mod clar și comunicate persoanei vizate, în conformitate cu obligațiile operatorului în ceea ce privește limitarea scopului și transparența. Evaluarea a ceea ce este „necesar” implică o evaluare combinată, bazată pe fapte privind prelucrarea „pentru obiectivul urmărit și privind caracterul său mai puțin intruziv comparativ cu alte opțiuni pentru îndeplinirea aceluiași scop”. Articolul 6 alineatul (1) litera (b) nu se referă la prelucrarea care este utilă, dar nu este necesară în mod obiectiv pentru prestarea serviciului contractual sau pentru luarea de măsuri precontractuale relevante la cererea persoanei vizate, chiar dacă aceasta este necesară în alte scopuri profesionale ale operatorului¹⁶.
18. După cum clarifică Orientările CEPD 2/2019, contractele nu pot extinde în mod artificial categoriile de date cu caracter personal sau tipurile de operațiuni de prelucrare pe care operatorul trebuie să le efectueze pentru executarea contractului în sensul articolului 6 alineatul (1) litera (b)¹⁷. Aceste orientări se referă, de asemenea, la cazurile în care pot apărea situații de tipul „take it or leave it” (acceptare sau renunțare) pentru persoanele vizate care pot fi interesate doar de unul dintre servicii. Acest lucru s-ar putea întâmpla atunci când un operator dorește să grupeze mai multe servicii sau elemente separate ale unui serviciu cu scopuri, caracteristici sau motivații fundamentale diferite într-un singur contract. În cazul în care contractul constă în mai multe servicii separate sau elemente ale unui serviciu care pot fi efectiv prestate în mod rezonabil independent unul de celălalt, aplicabilitatea articolului 6 alineatul (1) litera (b) ar trebui evaluată separat în contextul fiecăruia dintre aceste servicii, analizând ceea ce este necesar în mod obiectiv

¹⁴ Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, CEPD, pagina 8.

¹⁵ Idem.

¹⁶ Idem, pagina 7.

¹⁷ Idem, pagina 10.

pentru prestarea fiecăruia dintre serviciile individuale pe care persoana vizată l-a solicitat sau la care a aderat în mod activ¹⁸.

19. În conformitate cu orientările menționate anterior, operatorii trebuie să evalueze ceea ce este necesar în mod obiectiv pentru executarea contractului. În cazul în care operatorii nu pot demonstra că prelucrarea datelor privind contul de plăți cu caracter personal este necesară în mod obiectiv pentru prestarea separată a fiecăruia dintre aceste servicii, articolul 6 alineatul (1) litera (b) din RGPD nu este un temei juridic valabil pentru prelucrare. În aceste cazuri, operatorul ar trebui să ia în considerare un alt temei juridic pentru prelucrare.

2.3 Prevenirea fraudelor

20. În conformitate cu articolul 94 alineatul (1) din DSP2, statele membre permit prelucrarea datelor cu caracter personal de către sistemele de plată și prestatorii de servicii de plată în cazul în care este necesar pentru a garanta prevenirea, investigarea și detectarea fraudelor în domeniul plăților. Prelucrarea datelor cu caracter personal strict necesară în scopul prevenirii fraudelor ar putea constitui un interes legitim al prestatorului de servicii de plată în cauză, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate¹⁹. Activitățile de prelucrare în scopul prevenirii fraudelor ar trebui să se bazeze pe o evaluare atentă de la caz la caz de către operator, în conformitate cu principiul responsabilității. În plus, pentru a preveni fraudele, operatorii pot fi supuși, de asemenea, unor obligații legale specifice care impun prelucrarea datelor cu caracter personal.

2.4 Prelucrare ulterioară (PSIC și PSIP)

21. Articolul 6 alineatul (4) din RGPD stabilește condițiile de prelucrare a datelor cu caracter personal într-un alt scop decât cel pentru care au fost colectate. Mai precis, o astfel de prelucrare ulterioară poate avea loc, în cazul în care se întemeiază pe dreptul Uniunii sau dreptul intern, ceea ce constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 23 alineatul (1), în cazul în care persoana vizată și-a dat consimțământul sau în cazul în care prelucrarea într-un alt scop decât cel pentru care au fost colectate datele cu caracter personal este compatibilă cu scopul inițial.
22. Articolul 66 alineatul (3) litera (g) și articolul 67 alineatul (2) litera (f) din DSP2 trebuie luate în considerare cu atenție. Astfel cum s-a menționat mai sus, articolul 66 alineatul (3) litera (g) din DSP2 prevede că PSIP nu utilizează, nu accesează și nu stochează niciun fel de date în alte scopuri decât pentru prestarea serviciului de inițiere a plății solicitat în mod explicit de plătitor. Articolul 67 alineatul (2) litera (f) din DSP2 prevede că PSIC nu utilizează, nu accesează sau nu stochează niciun fel de date în alte scopuri decât pentru prestarea serviciului de informare cu privire la conturi, solicitat în mod explicit de către utilizatorul serviciilor de plată, în conformitate cu normele de protecție a datelor.
23. În consecință, articolul 66 alineatul (3) litera (g) și articolul 67 alineatul (2) litera (f) din DSP2 restricționează considerabil posibilitățile de prelucrare în alte scopuri, ceea ce înseamnă că prelucrarea în alt scop nu este permisă, cu excepția cazului în care persoana vizată și-a dat consimțământul în temeiul articolului 6 alineatul (1) litera (a) din RGPD sau prelucrarea este prevăzută de dreptul Uniunii sau de dreptul intern care se aplică operatorului, în temeiul articolului 6 alineatul (4) din RGPD. În cazul în care prelucrarea în alt scop decât cel pentru care au fost colectate datele cu caracter personal nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii

¹⁸ Idem, pagina 11.

¹⁹ Considerentul 47 din RGPD.

sau dreptul intern, restricțiile prevăzute la articolul 66 alineatul (3) litera (g) și la articolul 67 alineatul (2) litera (f) din DSP2 clarifică faptul că orice alt scop nu este compatibil cu scopul pentru care datele cu caracter personal au fost colectate inițial. Testul de compatibilitate prevăzut la articolul 6 alineatul (4) din RGPD nu poate avea drept rezultat un temei juridic pentru prelucrare.

24. Articolul 6 alineatul (4) din RGPD permite prelucrarea ulterioară în temeiul dreptului Uniunii sau al dreptului intern. De exemplu, toți PSIP și PSIC sunt entități care au obligații în temeiul articolului 3 alineatul (2) litera (a) din Directiva (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului (Directiva privind combaterea spălării banilor). Prin urmare, aceste entități obligate trebuie să aplice măsurile de precauție privind clientela, astfel cum se specifică în directivă. Datele cu caracter personal prelucrate în legătură cu un serviciu DSP2 sunt, prin urmare, prelucrate ulterior pe baza a cel puțin unei obligații legale care îi revine prestatorului de servicii²⁰.
25. Astfel cum se menționează la alineatul (20), articolul 6 alineatul (4) din RGPD indică faptul că prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate s-ar putea baza pe consimțământul persoanei vizate, dacă sunt îndeplinite toate condițiile pentru consimțământ în temeiul RGPD. Astfel cum s-a arătat mai sus, operatorul trebuie să demonstreze că este posibil ca persoana vizată să refuze sau să își retragă consimțământul fără a fi prejudiciată (considerentul 42 din RGPD).

2.5 Temeiul legal pentru acordarea accesului la cont (PSPSAC)

26. După cum s-a menționat la alineatul (10), utilizatorii serviciilor de plată își pot exercita dreptul de a utiliza serviciile de inițiere a plății și de informare cu privire la conturi. Obligațiile impuse statelor membre la articolul 66 alineatul (1) și la articolul 67 alineatul (1) din DSP2 ar trebui să fie transpuse în dreptul intern pentru a garanta aplicarea efectivă a dreptului utilizatorului serviciilor de plată de a beneficia de serviciile de plată menționate anterior. Aplicarea efectivă a acestor drepturi nu ar fi posibilă fără existența unei obligații corespunzătoare pentru PSPSAC, de obicei o bancă, de a acorda prestatorului de servicii de plată acces la cont cu condiția ca acesta să fi îndeplinit toate cerințele pentru a obține accesul la contul utilizatorului serviciilor de plată. În plus, articolul 66 alineatul (5) și articolul 67 alineatul (4) din DSP2 prevăd în mod clar că prestarea de servicii de inițiere a plății și de servicii de informare cu privire la conturi nu depinde de existența unei relații contractuale între PSIP/PSIC și PSPSAC.
27. Prelucrarea datelor cu caracter personal de către PSPSAC, care constă în acordarea accesului la datele cu caracter personal solicitate de PSIP și de PSIC pentru a-și presta serviciul de plată către utilizatorul serviciilor de plată, se bazează pe o obligație legală. Pentru a atinge obiectivele DSP2, PSPSAC trebuie să furnizeze datele cu caracter personal pentru serviciile PSIP și PSIC, ceea ce reprezintă o condiție necesară pentru ca PSIP și PSIC să își presteze serviciile și, astfel, să asigure drepturile prevăzute la articolul 66 alineatul (1) și la articolul 67 alineatul (1) din DSP2. Prin urmare, temeiul juridic aplicabil în acest caz este articolul 6 alineatul (1) litera (c) din RGPD.
28. Întrucât RGPD a precizat că prelucrarea pe baza unei obligații legale ar trebui să fie prevăzută în mod clar în dreptul Uniunii sau în dreptul intern [a se vedea articolul 6 alineatul (3) din RGPD], obligația prestatorilor de servicii de plată de a acorda acces ar trebui să rezulte din dreptul intern care transpune DSP2.

²⁰ Trebuie reținut că o examinare aprofundată pentru a stabili dacă Directiva privind combaterea spălării banilor respectă standardul prevăzut la articolul 6 alineatul (4) din RGPD nu intră în domeniul de aplicare al prezentului document.

3 CONSIMȚĂMÂNTUL EXPLICIT

3.1 Consimțământ în temeiul RGPD

29. În temeiul RGPD, consimțământul reprezintă unul dintre cele șase temeuri juridice pentru legalitatea prelucrării datelor cu caracter personal. Articolul 4 punctul 11 din RGPD definește consimțământul ca fiind „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate”; Aceste patru condiții, liber exprimate, specifice, informată și lipsite de ambiguitate, sunt esențiale pentru valabilitatea consimțământului. În conformitate cu Orientările CEPD 05/2020 privind consimțământul în temeiul Regulamentului (CE) 2016/679, consimțământul poate constitui un temei legal adecvat doar în cazul în care unei persoane vizate i se oferă controlul și i se dă posibilitatea reală de a face o alegere în ceea ce privește acceptarea sau refuzarea termenelor oferite sau respingerea acestora fără a fi prejudiciată. Atunci când solicită consimțământul, un operator are datoria de a evalua dacă cererea sa va îndeplini toate condițiile pentru obținerea unui consimțământ valabil. În cazul în care este obținut în deplină conformitate cu RGPD, consimțământul este un instrument care oferă persoanelor vizate posibilitatea de a controla dacă datele cu caracter personal care le privesc vor fi sau nu prelucrate. În caz contrar, controlul deținut de persoana vizată devine iluzoriu, iar consimțământul nu va constitui un temei juridic valabil pentru prelucrare, făcând ca activitatea de prelucrare să fie ilegală²¹.
30. De asemenea, sunt prevăzute garanții suplimentare în RGPD, la articolul 7, care prevede că operatorul de date trebuie să fie în măsură să demonstreze că a existat un consimțământ valabil la momentul prelucrării. De asemenea, cererea de consimțământ trebuie prezentată într-un mod care să poată fi distins în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. În plus, persoana vizată trebuie să fie informată cu privire la dreptul de a-și retrage consimțământul în orice moment, într-un mod la fel de simplu ca cel în care s-a acordat consimțământul.
31. În conformitate cu articolul 9 din RGPD, consimțământul este una dintre excepțiile de la interdicția generală pentru prelucrarea categoriilor speciale de date cu caracter personal. Cu toate acestea, în acest caz, consimțământul persoanei vizate trebuie să fie „explicit”²².
32. În conformitate cu Orientările CEPD 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, consimțământul explicit în temeiul RGPD se referă la modul în care acesta este exprimat de persoana vizată. Aceasta înseamnă că persoana vizată ar trebui să dea o declarație expresă de consimțământ pentru un scop (scopuri) specific(e) de prelucrare. O modalitate evidentă de a se asigura că un consimțământ este explicit ar fi confirmarea expresă a consimțământului într-o declarație scrisă. După caz, operatorul ar putea să se asigure că declarația scrisă este semnată de persoana vizată, pentru a elimina orice posibilă îndoială și potențială lipsă de dovezi în viitor.
33. Consimțământul nu poate fi în niciun caz dedus din declarații sau acțiuni potențial ambigue. De asemenea, un operator trebuie să fie conștient de faptul că nu se poate obține consimțământul

²¹ Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, CEPD, punctul 3.

²² A se vedea, de asemenea, Avizul 15/2011 privind definiția consimțământului (WP 187), p. 6-8 și/sau Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date în temeiul articolului 7 din Directiva 95/46/CE (WP 217), p. 9, 10, 13 și 14.

prin aceeași acțiune prin care se consimte la încheierea unui contract sau se acceptă termenii și condițiile generale ale unui serviciu.

3.2 Consimțământ în temeiul DSP2

34. CEPD ia act de complexitatea cadrului juridic privind consimțământul explicit, întrucât atât DSP2, cât și RGPD includ conceptul de „consimțământ explicit”. De aici apare întrebarea dacă noțiunea de „consimțământ explicit”, astfel cum este menționată la articolul 94 alineatul (2) din DSP2, ar trebui interpretată în același mod ca noțiunea de consimțământ explicit în temeiul RGPD.

3.2.1 Consimțământ explicit în temeiul articolului 94 alineatul (2) din DSP2

35. DSP2 include o serie de norme specifice privind prelucrarea datelor cu caracter personal, în special la articolul 94 alineatul (1) din DSP2, care stabilește că prelucrarea datelor cu caracter personal în sensul DSP2 trebuie să respecte legislația UE privind protecția datelor. În plus, articolul 94 alineatul (2) din DSP2 prevede că prestatorii de servicii de plată accesează, prelucrează și păstrează datele cu caracter personal necesare pentru furnizarea serviciilor lor de plată doar cu consimțământul explicit al utilizatorului serviciilor de plată. În conformitate cu articolul 33 alineatul (2) din DSP2, această cerință privind consimțământul explicit al utilizatorului serviciilor de plată nu se aplică PSIC. Cu toate acestea, articolul 67 alineatul (2) litera (a) din DSP2 prevede în continuare consimțământul explicit al PSIC pentru prestarea serviciului.
36. După cum s-a menționat mai sus, lista temeiurilor legale pentru prelucrare în temeiul RGPD este exhaustivă. Astfel cum se menționează la alineatul (14), temeiul juridic pentru prelucrarea datelor cu caracter personal în vederea prestării de servicii de plată este, în principiu, articolul 6 alineatul (1) litera (b) din RGPD, ceea ce înseamnă că prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a lua măsuri la cererea persoanei vizate înainte de încheierea unui contract. Rezultă că articolul 94 alineatul (2) din DSP2 nu poate fi considerat un temei juridic suplimentar pentru prelucrarea datelor cu caracter personal. CEPD consideră că, având în vedere cele de mai sus, prezentul alineat ar trebui interpretat, pe de o parte, în concordanță cu cadrul juridic aplicabil în materie de protecție a datelor și, pe de altă parte, într-un mod care păstrează efectul său util. Consimțământul explicit în temeiul articolului 94 alineatul (2) din DSP2 ar trebui, prin urmare, să fie considerat o cerință suplimentară de natură contractuală²³ în ceea ce privește accesul la datele cu caracter personal și prelucrarea ulterioară și stocarea acestora în scopul furnizării de servicii de plată și, prin urmare, nu este același lucru cu consimțământul (explicit) în temeiul RGPD.
37. „Consimțământul explicit” menționat la articolul 94 alineatul (2) din DSP2 este un consimțământ contractual. Aceasta implică faptul că articolul 94 alineatul (2) din DSP2 ar trebui interpretat în sensul că, atunci când încheie un contract cu un prestator de servicii de plată în temeiul DSP2, persoanele vizate trebuie să fie informate pe deplin cu privire la categoriile specifice de date cu caracter personal care vor fi prelucrate. În plus, acestea trebuie să fie informate cu privire la scopul specific (serviciul de plată) pentru care vor fi prelucrate datele lor cu caracter personal și trebuie să fie de acord în mod explicit cu aceste clauze. Astfel de clauze ar trebui să poată fi distinse în mod clar de celelalte aspecte abordate în contract și ar trebui să fie acceptate în mod explicit de persoana vizată.
38. Elementul central al noțiunii de „consimțământ explicit” prevăzute la articolul 94 alineatul (2) din DSP2 este obținerea accesului la datele cu caracter personal pentru prelucrarea și stocarea

²³ Scrisoarea CEPD cu privire la Directiva DSP2, 5 iulie 2018, pagina 4.

ulterioară a acestora în scopul prestării de servicii de plată. Aceasta înseamnă că prestatorul de servicii de plată²⁴ nu prelucrează încă datele cu caracter personal, ci are nevoie de acces la datele cu caracter personal care au fost prelucrate sub responsabilitatea oricărui alt operator. În cazul în care un utilizator al serviciilor de plată încheie un contract, de exemplu, cu un prestator de servicii de inițiere a plății, acest prestator trebuie să obțină acces la datele cu caracter personal ale utilizatorului de servicii de plată care sunt prelucrate sub responsabilitatea prestatorului de servicii de plată care oferă servicii de administrare cont. Obiectul consimțământului explicit prevăzut la articolul 94 alineatul (2) din DSP2 este permisiunea de a obține acces la datele cu caracter personal respective, pentru a putea prelucra și stoca aceste date cu caracter personal care sunt necesare în scopul prestării serviciului de plată. În cazul în care persoana vizată își dă consimțământul explicit, prestatorul de servicii de plată care oferă servicii de administrare cont este obligat să permită accesul la datele cu caracter personal indicate.

39. Deși consimțământul prevăzut la articolul 94 alineatul (2) din DSP2 nu este un temei juridic pentru prelucrarea datelor cu caracter personal, acest consimțământ este legat în mod specific de protecția datelor cu caracter personal și de protecția datelor și asigură transparența și un anumit grad de control pentru utilizatorul serviciilor de plată²⁵. Deși DSP2 nu specifică condițiile de fond pentru consimțământ în temeiul articolului 94 alineatul (2) din DSP2, acesta ar trebui, astfel cum s-a menționat mai sus, să fie înțeles în concordanță cu cadrul juridic aplicabil privind protecția datelor și într-un mod care să mențină efectul util al acestuia.
40. În ceea ce privește informațiile care trebuie furnizate de operatori și cerința de transparență, Orientările Grupului de lucru „Articolul 29” privind transparența specifică faptul că *„un element esențial al principiului transparenței subliniat în aceste dispoziții este că persoana vizată ar trebui să fie în măsură să determine dinainte domeniul de aplicare și consecințele prelucrării și că aceasta nu ar trebui luată prin surprindere la un moment ulterior cu privire la modul în care au fost utilizate datele sale cu caracter personal”*²⁶.
41. În plus, în conformitate cu principiul limitării legate de scop, datele cu caracter personal trebuie colectate în scopuri specificate, explicite și legitime [articolul 5 alineatul (1) litera (b) din RGPD]. În cazul în care datele cu caracter personal sunt colectate în mai multe scopuri, „operatorii ar trebui să evite identificarea unui singur scop larg pentru a justifica diferite activități de prelucrare ulterioare care, de fapt, sunt legate într-o măsură foarte mică de scopul inițial efectiv”²⁷. CEPD a subliniat, cel mai recent în contextul contractelor de servicii online, riscul includerii în contracte a unor clauze generale de prelucrare și a afirmat că scopul colectării trebuie să fie identificat în mod clar și specific: trebuie să fie suficient de detaliat pentru a determina tipul de prelucrare și nu este inclus în scopul specificat, precum și pentru a permite evaluarea respectării legii și aplicarea garanțiilor privind prelucrarea datelor²⁸.
42. Atunci când este luat în considerare în contextul cerinței suplimentare privind consimțământul explicit în temeiul articolului 94 alineatul (2) din DSP2, acest lucru implică faptul că operatorii

²⁴ Acest lucru este valabil pentru serviciile 1-7 din anexa 1 la DSP2.

²⁵ Articolul 94 alineatul (2) din DSP2 se încadrează la capitolul 4 „Protecția datelor”.

²⁶ Grupul de lucru „Articolul 29”, Orientări privind transparența în temeiul Regulamentului 2016/679, alineatul (10) (adoptate la 11 aprilie 2018) – aprobate de CEPD.

²⁷ Avizul 03/2013 al Grupului de lucru „Articolul 29” privind limitarea scopului (WP 203), pagina 16.

²⁸ Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, punctul 16 (versiunea privind consultarea publică) și Avizul 03/2013 al Grupului de lucru „Articolul 29” privind limitarea scopului (WP203), paginile 15-16.

trebuie să furnizeze persoanelor vizate informații specifice și explicite cu privire la scopurile specifice identificate de operator pentru care datele lor cu caracter personal sunt accesate, prelucrate și păstrate. În conformitate cu articolul 94 alineatul (2) din DSP2, persoanele vizate trebuie să accepte în mod explicit aceste scopuri specifice.

43. În plus, astfel cum s-a arătat mai sus la punctul 10, CEPD subliniază că utilizatorul serviciilor de plată trebuie să poată alege dacă să utilizeze sau nu serviciul și nu poate fi obligat să facă acest lucru. Prin urmare, consimțământul în temeiul articolului 94 alineatul (2) din DSP2 trebuie să fie, de asemenea, un consimțământ exprimat în mod liber.

3.3 Concluzie

44. Consimțământul explicit în temeiul DSP2 este diferit de consimțământul (explicit) în temeiul RGPD. Consimțământul explicit în temeiul articolului 94 alineatul (2) din DSP2 este o cerință suplimentară de natură contractuală. În cazul în care un prestator de servicii de plată are nevoie de acces la date cu caracter personal pentru prestarea unui serviciu de plată, este necesar consimțământul explicit al utilizatorului serviciilor de plată, în conformitate cu articolul 94 alineatul (2) din DSP2.

4 PRELUCRAREA DATELOR PĂRȚILOR PASIVE

4.1 Datele părților pasive

45. O problemă de protecție a datelor care necesită o atenție deosebită este prelucrarea așa-numitelor „date ale părților pasive”. În contextul prezentului document, datele părților pasive sunt date cu caracter personal referitoare la o persoană vizată care nu este utilizatorul unui anumit prestator de servicii de plată, dar ale cărei date cu caracter personal sunt prelucrate de respectivul prestator de servicii de plată în vederea executării unui contract între prestator și utilizatorul serviciilor de plată. De exemplu, acesta este cazul în care un utilizator de servicii de plată, persoana vizată A, utilizează serviciile unui PSIC, iar persoana vizată B a efectuat o serie de operațiuni de plată în contul de plăți al persoanei vizate A. În acest caz, persoana vizată B este considerată „parte pasivă”, iar datele cu caracter personal (cum ar fi numărul de cont al persoanei vizate B și suma de bani care a fost implicată în aceste operațiuni) referitoare la persoana vizată B sunt considerate „date ale părții pasive”.

4.2 Interesul legitim al operatorului

46. Articolul 5 alineatul (1) litera (b) din RGPD prevede că datele cu caracter personal sunt colectate numai în scopuri determinate, explicite și legitime și nu pot fi prelucrate ulterior într-un mod incompatibil cu aceste scopuri. În plus, RGPD prevede că orice prelucrare a datelor cu caracter personal trebuie să fie atât necesară, cât și proporțională și în conformitate cu principiile de protecție a datelor, cum ar fi cele privind limitarea scopului și reducerea la minimum a datelor.

47. RGPD poate permite prelucrarea datelor părților pasive atunci când această prelucrare este necesară în scopul intereselor legitime urmărite de un operator sau de o parte terță [articolul 6 alineatul (1) litera (f) din RGPD]. Cu toate acestea, o astfel de prelucrare poate avea loc numai atunci când asupra interesului legitim al operatorului nu „prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecția datelor cu caracter personal”.

48. Prin urmare, un temei legal pentru prelucrarea datelor părților pasive de către PSIP și PSIC – în contextul prestării de servicii de plată în temeiul DSP2 – ar putea fi interesul legitim al unui operator sau al unui terț de a executa contractul cu utilizatorul serviciilor de plată. Necesitatea de a prelucra datele cu caracter personal ale părții pasive este limitată și determinată de așteptările rezonabile ale acestor persoane vizate. În contextul prestării de servicii de plată care intră sub incidența DSP2, trebuie instituite măsuri eficiente și adecvate pentru a garanta că asupra intereselor sau drepturilor și libertăților fundamentale ale părților pasive nu prevalează alte interese și pentru a asigura respectarea așteptărilor rezonabile ale acestor persoane vizate cu privire la prelucrarea datelor lor cu caracter personal. În acest sens, operatorul (PSIC sau PSIP) trebuie să stabilească garanțiile necesare pentru prelucrare în vederea protejării drepturilor persoanelor vizate. Aceasta include măsuri tehnice pentru a asigura că datele părților pasive nu sunt prelucrate în alt scop decât scopul pentru care datele cu caracter personal au fost colectate inițial de PSIP și PSIC. Dacă este fezabil, ar trebui aplicate și tehnici de criptare sau alte tehnici pentru a obține un nivel adecvat de securitate și reducerea la minimum a datelor.

4.3 Prelucrarea ulterioară a datelor cu caracter personal ale părții pasive

49. Astfel cum se menționează la punctul 29, datele cu caracter personal prelucrate în legătură cu un serviciu de plată reglementat de DSP2 ar putea fi prelucrate ulterior pe baza obligațiilor legale care revin prestatorului de servicii. Aceste obligații legale s-ar putea referi la datele cu caracter personal ale părții pasive.

50. În ceea ce privește prelucrarea ulterioară a datelor părților pasive pe baza interesului legitim, CEPD este de părere că aceste date nu pot fi utilizate în alt scop decât cel pentru care au fost colectate datele cu caracter personal, altul în temeiul dreptului UE sau al dreptului intern. Consimțământul părții pasive nu este fezabil din punct de vedere juridic, deoarece, pentru a obține consimțământul, datele cu caracter personal ale părții pasive ar trebui să fie colectate sau prelucrate, lucru pentru care nu există niciun temei juridic la articolul 6 din RGPD. Nici testul de compatibilitate prevăzut la articolul 6 alineatul (4) din RGPD nu poate oferi un motiv pentru prelucrarea în alte scopuri (de exemplu, activități de marketing direct). Drepturile și libertățile acestor persoane vizate care sunt părți pasive nu vor fi respectate dacă noul operator de date utilizează datele cu caracter personal în alte scopuri, ținând seama de contextul în care au fost colectate datele cu caracter personal, în special de absența oricărei relații cu persoanele vizate care sunt părți pasive²⁹; absența oricărei legături între orice alt scop și scopul în care au fost colectate inițial datele cu caracter personal (și anume, faptul că PSP au nevoie doar de datele părții pasive pentru a executa un contract cu cealaltă parte contractantă); natura datelor cu caracter personal implicate³⁰, faptul că persoanele vizate nu sunt în măsură să se aștepte în mod rezonabil la o prelucrare ulterioară sau chiar să știe care operator poate prelucra datele lor cu caracter personal și având în vedere restricțiile legale privind prelucrarea prevăzute la articolul 66 alineatul (3) litera (g) și la articolul 67 alineatul (2) litera (f) din DSP2.

²⁹ Considerentul 87 din DSP2 prevede că DSP2 se referă numai la „obligațiile și responsabilitățile contractuale dintre utilizatorul serviciilor de plată și prestatorul de servicii de plată”. Prin urmare, datele părților pasive nu intră în domeniul de aplicare al DSP2.

³⁰ Ar trebui acordată o atenție deosebită prelucrării datelor financiare cu caracter personal, deoarece se poate considera că prelucrarea crește riscul posibil pentru drepturile și libertățile persoanelor fizice, în conformitate cu Orientările privind evaluarea impactului asupra protecției datelor (EIPD).

5 PRELUCRAREA CATEGORIILOR SPECIALE DE DATE CU CARACTER PERSONAL ÎN TEMEIUL DSP2

5.1 Categoriile speciale de date cu caracter personal

51. Articolul 9 alineatul (1) din RGPD interzice prelucrarea de „date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice”.
52. Ar trebui subliniat faptul că, în unele state membre, plățile electronice sunt deja omniprezente și sunt preferate de multe persoane în locul folosirii numerarului în operațiunile lor zilnice. În același timp, tranzacțiile financiare pot dezvălui informații sensibile cu privire la o persoană vizată, inclusiv cele legate de categorii speciale de date cu caracter personal. De exemplu, în funcție de detaliile operațiunii, pot fi dezvăluite opiniile politice și convingerile religioase ale persoanelor judecând după donațiile efectuate către partide sau organizații politice, biserici sau parohii. Apartenența la un sindicat poate fi dezvăluită prin deducerea unei cotizații anuale de membru din contul bancar al unei persoane. Datele cu caracter personal privind sănătatea pot fi colectate din analiza facturilor medicale plătite de o persoană vizată unui profesionist din domeniul medical (de exemplu, un psihiatru). În cele din urmă, informațiile privind anumite achiziții pot dezvălui informații privind viața sexuală sau orientarea sexuală a unei persoane. După cum arată aceste exemple, chiar și operațiunile individuale pot conține categorii speciale de date cu caracter personal. În plus, serviciile de informare cu privire la conturi s-ar putea baza pe crearea de profiluri, astfel cum este definită la articolul 4 punctul 4 din RGPD. După cum s-a menționat anterior în Orientările Grupului de lucru „Articolul 29” privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679, astfel cum a fost aprobat de CEPD, „crearea de profiluri poate crea o categorie specială de date prin deducție din date care nu reprezintă o categorie specială de date de sine stătătoare, dar care devin astfel de date atunci când sunt combinate cu altele”³¹. Aceasta înseamnă că, prin însumarea tranzacțiilor financiare, pot fi dezvăluite diferite tipuri de comportament, care pot include categorii speciale de date cu caracter personal. Prin urmare, șansele ca un prestator de servicii care prelucrează informații privind tranzacțiile financiare ale persoanelor vizate să prelucreze, de asemenea, categorii speciale de date cu caracter personal sunt considerabile.
53. În ceea ce privește noțiunea de „date sensibile privind plățile”, CEPD observă următoarele. Definiția datelor sensibile privind plățile din DSP2 diferă considerabil de modul în care se utilizează noțiunea de „date cu caracter personal sensibile” în mod obișnuit în contextul RGPD și al protecției datelor (legislație). În cazul în care DSP2 definește „datele sensibile privind plățile” ca fiind „date, inclusiv elemente de securitate personalizate, care pot fi utilizate în scopul fraudării”, RGPD subliniază necesitatea unei protecții specifice a categoriilor speciale de date cu caracter personal care, în temeiul articolului 9 din RGPD și prin natura lor, sunt deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale, cum ar fi categoriile speciale de date cu caracter personal³². În acest sens, se recomandă cel puțin să se cartografieze și să se clasifice cu precizie ce

³¹ Grupul de lucru „Articolul 29” pentru protecția datelor, Orientări privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP251rev.01, pagina 15.

³² De exemplu, la considerentul 10 din RGPD, categoriile speciale de date cu caracter personal sunt denumite „date sensibile”.

tip de date cu caracter personal vor fi prelucrate. Cel mai probabil, va fi necesară o evaluare a impactului asupra protecției datelor (EIPD) în conformitate cu articolul 35 din RGPD, care va contribui la acest exercițiu de cartografiere. Mai multe orientări privind EIPD pot fi găsite în Orientările Grupului de lucru „Articolul 29” privind evaluarea impactului asupra protecției datelor (EIPD) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679, astfel cum au fost aprobate de CEPD.

5.2 Derogări posibile

54. Interdicția prevăzută la articolul 9 din RGPD nu este absolută. În special, întrucât derogările de la articolul 9 alineatul (2) literele (b)–(f) și (h)–(j) din RGPD nu sunt în mod evident aplicabile prelucrării datelor cu caracter personal în contextul DSP2, ar putea fi avute în vedere următoarele două derogări de la articolul 9 alineatul (2) din RGPD:
- a) Interdicția nu se aplică în cazul în care persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specificate [articolul 9 alineatul (2) litera (a) din RGPD].
 - b) Interdicția nu se aplică dacă prelucrarea este necesară din motive de interes public major, în temeiul dreptului Uniunii sau al dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate [articolul 9 alineatul (2) litera (g) din RGPD].
55. Ar trebui subliniat faptul că lista derogărilor prevăzute la articolul 9 alineatul (2) din RGPD este exhaustivă. Posibilitatea includerii categoriilor speciale de date cu caracter personal în datele cu caracter personal prelucrate pentru furnizarea oricăruia dintre serviciile care intră sub incidența DSP2 trebuie să fie recunoscută de prestatorul de servicii. Întrucât interdicția prevăzută la articolul 9 alineatul (1) din RGPD se aplică acestor prestatori de servicii, aceștia trebuie să se asigure că li se aplică una dintre excepțiile prevăzute la articolul 9 alineatul (2) din RGPD. Ar trebui subliniat faptul că, în cazul în care prestatorul de servicii nu poate demonstra că una dintre derogări este îndeplinită, se aplică interdicția prevăzută la articolul 9 alineatul (1).

5.3 Interesul public major

56. Serviciile de plată pot prelucra categorii speciale de date cu caracter personal din motive de interes public major, dar numai atunci când sunt îndeplinite toate condițiile prevăzute la articolul 9 alineatul (2) litera (g) din RGPD. Aceasta înseamnă că prelucrarea categoriilor speciale de date cu caracter personal trebuie să fie abordată printr-o derogare specifică de la articolul 9 alineatul (1) din RGPD în dreptul Uniunii sau în dreptul intern. Această dispoziție va trebui să abordeze proporționalitatea în raport cu obiectivul urmărit al prelucrării și să conțină măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate. În plus, această dispoziție din dreptul Uniunii sau dreptul intern va trebui să respecte esența dreptului la protecția datelor. În cele din urmă, prelucrarea categoriilor speciale de date trebuie să fie, de asemenea, demonstrată ca fiind necesară din motive legate de interesul public major, inclusiv de interese de importanță sistemică. Numai atunci când toate aceste condiții sunt îndeplinite integral, această derogare ar putea deveni aplicabilă tipurilor de servicii de plată desemnate.

5.4 Consimțământul explicit

57. În cazurile în care derogarea prevăzută la articolul 9 alineatul (2) litera (g) din RGPD nu se aplică, obținerea consimțământului explicit în conformitate cu condițiile de valabilitate a consimțământului prevăzute în RGPD pare să rămână singura derogare legală posibilă pentru prelucrarea de către PT a unor categorii speciale de date cu caracter personal. Orientările CEPD 05/2020 privind consimțământul în temeiul Regulamentului 2016/679 prevăd³³ că: „Articolul 9 alineatul (2) nu recunoaște situația în care prelucrarea este «necesară pentru executarea unui contract» ca o excepție de la interdicția generală de a prelucra categorii speciale de date. Prin urmare, operatorii și statele membre care se regăsesc în această situație ar trebui să examineze excepțiile specifice prevăzute la articolul 9 alineatul (2) literele (b)–(j). Atunci când prestatorii de servicii se bazează pe articolul 9 alineatul (2) litera (a) din RGPD, aceștia trebuie să se asigure că li s-a acordat consimțământul explicit înainte de începerea prelucrării.” Consimțământul explicit, astfel cum este prevăzut la articolul 9 alineatul (2) litera (a) din RGPD, trebuie să îndeplinească toate cerințele prevăzute de RGPD.

5.5 Nicio derogare adecvată

58. Astfel cum s-a menționat mai sus, în cazul în care prestatorul de servicii nu poate demonstra că una dintre derogări este îndeplinită, se aplică interdicția prevăzută la articolul 9 alineatul (1). În acest caz, ar putea fi instituite măsuri tehnice pentru a preveni prelucrarea unor categorii speciale de date cu caracter personal, de exemplu prin prevenirea prelucrării anumitor puncte de date. În acest sens, prestatorii de servicii de plată pot explora posibilitățile tehnice de a exclude categorii speciale de date cu caracter personal și de a permite accesul selectat, ceea ce ar împiedica prelucrarea de către PT a unor categorii speciale de date cu caracter personal referitoare la părțile pasive.

³³ Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, CEPD, punctul 99.

6 REDUCEREA LA MINIMUM A DATELOR, SECURITATEA, TRANSPARENȚA, RESPONSABILITATEA ȘI CREAREA DE PROFILURI

6.1 Reducerea la minimum a datelor și protecția datelor începând cu momentul conceperii și în mod implicit

59. Principiul reducerii la minimum a datelor este consacrat la articolul 5 alineatul (1) litera (c) din RGPD: „Datele cu caracter personal sunt [...] adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate”. În esență, în temeiul principiului reducerii la minimum a datelor, operatorii nu ar trebui să prelucreze mai multe date cu caracter personal decât este necesar pentru atingerea scopului specific în cauză. Astfel cum s-a subliniat în capitolul 2, cuantumul și tipul de date cu caracter personal necesare pentru prestarea serviciului de plată sunt determinate de obiectivul și de scopul contractual înțeles de comun acord³⁴. Reducerea la minimum a datelor este aplicabilă fiecărei prelucrări (de exemplu, fiecare colectare sau acces la date cu caracter personal și fiecare cerere de astfel de date). Orientările CEPD nr. 4/2019 privind articolul 25 (Protecția datelor începând cu momentul conceperii și în mod implicit) (PDMCMI) prevăd că „persoanele împuternicite de către operatori și furnizorii de tehnologie sunt, de asemenea, recunoscuți drept factori-cheie pentru PDMCMI, iar aceștia ar trebui, de asemenea, să fie conștienți de faptul că operatorii au obligația de a prelucra date cu caracter personal numai cu ajutorul unor sisteme și tehnologii care beneficiază de o protecție integrată a datelor”³⁵.
60. Articolul 25 din RGPD conține obligațiile de a aplica protecția datelor începând cu momentul conceperii și în mod implicit. Aceste obligații sunt deosebit de importante pentru principiul reducerii la minimum a datelor. Acest articol stabilește că operatorii, atât în momentul stabilirii mijloacelor de prelucrare, cât și în momentul prelucrării propriu-zise, pun în aplicare măsuri tehnice și organizatorice adecvate, care sunt concepute pentru a pune în aplicare principiile de protecție a datelor în mod eficace și pentru a integra garanțiile necesare în prelucrare pentru a îndeplini cerințele RGPD și a proteja drepturile persoanelor vizate. Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. Aceste măsuri pot include criptarea, pseudonimizarea și alte măsuri tehnice.
61. Atunci când se aplică obligația prevăzută la articolul 25 din RGPD, stadiul actual al tehnologiei, costul punerii în aplicare și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea sunt elementele care trebuie luate în considerare. Clarificări suplimentare cu privire la această obligație sunt oferite în Orientările nr. 4/2019 ale CEPD menționate mai sus privind articolul 25 (Protecția datelor începând cu momentul conceperii și în mod implicit).

6.2 Măsuri de reducere la minimum a datelor

62. Prestatorii terți (PT) care accesează datele privind conturile de plăți pentru a furniza serviciile solicitate trebuie, de asemenea, să țină seama de principiul reducerii la minimum a datelor și

³⁴ Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, CEPD, punctul 32.

³⁵ Orientările 4/2019 privind articolul 25 Protecția datelor începând cu momentul conceperii și în mod implicit, pagina 29.

trebuie să colecteze numai datele cu caracter personal necesare pentru furnizarea serviciilor de plată specifice solicitate de utilizatorul serviciilor de plată. În principiu, accesul la datele cu caracter personal ar trebui să se limiteze la ceea ce este necesar pentru prestarea de servicii de plată. Astfel cum s-a arătat în capitolul 2, DSP2 impune PSPSAC să partajeze informațiile privind utilizatorii serviciilor de plată la cererea utilizatorului serviciilor de plată, atunci când utilizatorul serviciilor de plată dorește să utilizeze un serviciu de inițiere a plății sau un serviciu de informare cu privire la conturi.

63. Atunci când nu sunt necesare toate datele privind conturile de plăți pentru executarea contractului, PSIC ar trebui să facă o selecție a categoriilor de date relevante înainte de colectarea datelor. De exemplu, categoriile de date care ar putea să nu fie necesare pot include identitatea părții pasive și caracteristicile operațiunii. De asemenea, cu excepția cazului în care dreptul intern sau al UE prevede acest lucru, este posibil ca IBAN-ul corespunzător contului bancar al părții pasive să nu fie afișat.
64. În acest sens, ar putea fi luată în considerare posibila aplicare a unor măsuri tehnice care permit sau sprijină prestatorii terți în ceea ce privește obligația lor de a accesa și de a extrage numai datele cu caracter personal necesare pentru furnizarea serviciilor lor, ca parte a punerii în aplicare a unor politici adecvate de protecție a datelor, în conformitate cu articolul 24 alineatul (2) din RGPD. În acest sens, CEPD recomandă utilizarea instrumentelor digitale pentru a sprijini PSIC în ceea ce privește obligația lor de a colecta numai date cu caracter personal care sunt necesare pentru scopurile în care sunt prelucrate. De exemplu, atunci când un prestator de servicii nu are nevoie de caracteristicile tranzacției (în câmpul de descriere al înregistrărilor operațiunilor) pentru furnizarea serviciului său, un instrument de selecție digitală ar putea funcționa ca mijloc prin care PT să poată exclude acest câmp din operațiunile lor globale de prelucrare.

Exemplul 2:

HappyPayments, prestatorul nostru de servicii de informare cu privire la conturi din exemplul 1, dorește să se asigure că prelucrează numai datele cu caracter personal aferente contului de plăți de care sunt interesați utilizatorii săi. Solicitarea accesului la mai multe date privind conturile de plăți nu ar fi necesară pentru prestarea serviciului. Prin urmare, permite utilizatorilor să selecteze tipurile specifice de informații care îi interesează.

Utilizatorul A dorește o imagine de ansamblu asupra cheltuielilor sale din ultimele două luni. Astfel, acesta solicită pentru cele două conturi bancare ale sale, deținute la doi PSPSAC diferiți, informații privind toate operațiunile din ultimele două luni, valoarea operațiunilor, data executării și numele destinatarului, și bifează căsuțele corespunzătoare din interfața pentru utilizatori a HappyPayments.

HappyPayments solicită apoi de la PSPSAC respectivi numai informațiile corespunzătoare câmpurilor stabilite de utilizatorul A și numai pentru perioada ultimelor două luni. Nu se solicită informații precum „comunicarea” transferului sau chiar codul IBAN, întrucât utilizatorul A nu a solicitat aceste informații.

Pentru a permite HappyPayments să își respecte obligațiile de reducere la minimum a datelor, PSPSAC permit HappyPayments să solicite câmpuri specifice pentru o serie de date.

65. În acest sens, ar trebui remarcat, de asemenea, faptul că, în temeiul DSP2, PSPSAC au doar dreptul de a oferi acces la informațiile privind conturile de plăți. DSP2 nu cuprinde niciun temei juridic pentru a oferi acces la datele cu caracter personal conținute în alte conturi, cum ar fi conturile de economii, creditele ipotecare sau conturile de investiții. În consecință, în temeiul DSP2, trebuie puse în aplicare măsuri tehnice pentru a se asigura că accesul este limitat la informațiile necesare privind contul de plăți.

66. Pe lângă colectarea unui număr cât mai mic de date, prestatorul de servicii trebuie, de asemenea, să pună în aplicare perioade de păstrare limitate. Datele cu caracter personal nu ar trebui stocate de prestatorul de servicii pe o perioadă mai lungă decât este necesar în raport cu scopurile solicitate de utilizatorul serviciilor de plată.
67. În cazul în care contractul dintre persoana vizată și PSIC necesită transmiterea de date cu caracter personal către terți, atunci pot fi transmise numai acele date cu caracter personal care sunt necesare pentru executarea contractului. Persoanele vizate ar trebui, de asemenea, să fie informate în mod specific cu privire la transmitere și la datele cu caracter personal care urmează să fie transmise acestei părți terțe.

6.3 Securitate

68. CEPD a subliniat deja că încălcarea datelor financiare cu caracter personal „*implică în mod clar efecte grave în viața de zi cu zi a persoanei vizate*” și citează ca exemplu riscurile de fraudă în domeniul plăților³⁶.
69. În cazul în care o încălcare a securității datelor implică date financiare, persoana vizată poate fi expusă unor riscuri considerabile. În funcție de informațiile divulgate, persoanele vizate pot fi expuse riscului de furt de identitate, de furt de fonduri din conturile lor și de alte active. În plus, există posibilitatea ca expunerea datelor privind operațiunile să presupună riscuri considerabile la adresa vieții private, întrucât datele privind operațiunile pot conține trimiteri la toate aspectele vieții private a unei persoane vizate. În același timp, datele financiare sunt în mod evident valoroase pentru infractori și, prin urmare, reprezintă un obiectiv atractiv.
70. În calitate de operatori, prestatorii de servicii de plată sunt obligați să ia măsuri adecvate pentru a proteja datele cu caracter personal ale persoanelor vizate [articolul 24 alineatul (1) din RGPD]. Cu cât riscurile asociate activității de prelucrare efectuate de operator sunt mai ridicate, cu atât mai ridicate trebuie să fie și standardele de securitate aplicate. Întrucât prelucrarea datelor financiare este legată de o gamă largă de riscuri grave, și măsurile de securitate ar trebui să fie, în consecință, ridicate.
71. Prestatorii de servicii ar trebui să respecte standarde înalte, inclusiv mecanismele stricte de autentificare a clienților și standarde înalte de securitate pentru echipamentele tehnice³⁷. Alte proceduri, cum ar fi verificarea respectării de către persoanele împuternicite de operator a standardelor de securitate și a procedurilor de punere în aplicare împotriva accesului neautorizat, sunt, de asemenea, importante.

6.4 Transparență și răspundere

72. Transparența și răspunderea sunt două principii fundamentale prevăzute de RGPD.
73. În ceea ce privește transparența [articolul 5 alineatul (1) litera (a) din RGPD], articolul 12 din RGPD prevede că operatorii iau măsurile adecvate pentru a furniza orice informații menționate la articolele 13 și 14 din RGPD. În plus, acesta impune ca informațiile sau comunicarea cu privire la prelucrarea datelor cu caracter personal să fie concise, transparente, inteligibile și ușor accesibile. Informațiile trebuie să fie prezentate într-un limbaj clar și simplu și în scris „sau prin alte mijloace, inclusiv, după caz, prin mijloace electronice”. Orientările Grupului de lucru „Articolul 29” privind

³⁶ Orientările Grupului de lucru „Articolul 29” privind evaluarea impactului asupra protecției datelor (EIPD) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679, WP248 rev.01 - aprobate de CEPD.

³⁷ A se vedea STR.

transparența în temeiul Regulamentului 2016/679, astfel cum a fost aprobate de CEPD, oferă îndrumări specifice pentru respectarea principiului transparenței în mediile digitale.

74. În conformitate cu orientările menționate anterior privind transparența în temeiul Regulamentului (UE) 2016/679, articolul 11 din RGPD ar trebui interpretat ca o modalitate de a asigura reducerea reală la minimum a datelor fără a împiedica exercitarea drepturilor persoanelor vizate, iar exercitarea drepturilor persoanei vizate ar trebui să fie posibilă cu ajutorul informațiilor suplimentare furnizate de persoana vizată. Pot exista situații în care un operator prelucrează date cu caracter personal care nu necesită identificarea unei persoane vizate (de exemplu, în cazul datelor pseudonimizate). În astfel de cazuri, articolul 11 alineatul (1) poate fi, de asemenea, relevant, deoarece prevede că un operator nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării RGPD.
75. Pentru serviciile prevăzute în DSP2, articolul 13 din RGPD se aplică datelor cu caracter personal colectate de la persoana vizată, iar articolul 14 se aplică în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată.
76. În special, persoana vizată trebuie să fie informată cu privire la perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, cu privire la criteriile utilizate pentru a stabili perioada respectivă și, după caz, cu privire la interesele legitime urmărite de operator sau de o posibilă parte terță. În cazul în care prelucrarea se bazează pe consimțământ, astfel cum se menționează la articolul 6 alineatul (1) litera (a) din RGPD, sau pe consimțământul explicit, astfel cum se menționează la articolul 9 alineatul (2) litera (a) din RGPD, persoana vizată trebuie să fie informată în orice moment cu privire la existența dreptului de a-și retrage consimțământul.
77. Operatorul furnizează informațiile persoanei vizate, având în vedere circumstanțele specifice în care sunt prelucrate datele cu caracter personal. În cazul în care datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată³⁸, situație probabilă în cazul PSIC, informațiile trebuie furnizate cel târziu în momentul primei comunicări către persoana vizată. În cazul în care datele cu caracter personal urmează să fie divulgate unui alt destinatar, informațiile trebuie furnizate cel târziu în momentul în care datele cu caracter personal sunt divulgate pentru prima dată.
78. În ceea ce privește serviciile de plată online, orientările menționate mai sus clarifică faptul că operatorii de date pot aplica o abordare stratificată atunci când optează să utilizeze o combinație de metode pentru a asigura transparența. Se recomandă, în special, ca declarațiile/anunțurile de confidențialitate stratificate să fie utilizate pentru a face legătura cu diferitele categorii de informații care trebuie furnizate persoanei vizate, în loc să se afișeze toate aceste informații într-un singur anunț pe un ecran, pentru a se evita oboseala informațională și, în același timp, pentru a se asigura eficacitatea informațiilor.
79. Orientările menționate anterior clarifică, de asemenea, faptul că operatorii pot alege să utilizeze instrumente suplimentare pentru a furniza informații persoanei vizate, cum ar fi panourile privind confidențialitatea. Un panou privind confidențialitatea constituie un punct unic unde persoanele vizate pot vizualiza „informații despre confidențialitate” și gestiona preferințele lor în materie de confidențialitate prin faptul că permit sau împiedică utilizarea datelor lor în anumite moduri de

³⁸ Articolul 14 alineatul (3) litera (b) din RGPD.

către operatorul în cauză³⁹. Un panou privind confidențialitatea ar putea oferi o imagine de ansamblu a prestatorilor terți care au obținut consimțământul explicit al persoanelor vizate și ar putea oferi, de asemenea, informații relevante privind natura și cantitatea datelor cu caracter personal care au fost accesate de prestatorii terți. În principiu, un PPSAC poate oferi utilizatorului posibilitatea de retragere a unui consimțământ specific explicit în temeiul DSP2⁴⁰ prin intermediul prezentării generale, ceea ce ar duce la refuzarea accesului la conturile lor de plăți pentru unul sau mai mulți PT. De asemenea, utilizatorul ar putea solicita unui PPSAC să refuze accesul la contul (conturile) său (lor) de plăți pentru unul sau mai mulți prestatorii terți specifici⁴¹, deoarece acesta este dreptul utilizatorului de a (nu) utiliza un serviciu de informare cu privire la conturi. În cazul în care panourile privind confidențialitatea sunt utilizate pentru a acorda sau a retrage un consimțământ explicit, acestea ar trebui să fie concepute și aplicate în mod legal și, în special, să prevină crearea de obstacole în calea dreptului prestatorilor terți de a presta servicii în conformitate cu DSP2. În acest sens și în conformitate cu dispozițiile aplicabile din DSP2, un PT are posibilitatea de a obține din nou consimțământul explicit din partea utilizatorului după retragerea acestui consimțământ.

80. Principiile răspunderii impun operatorului să stabilească măsuri tehnice și organizatorice adecvate pentru a asigura și a fi în măsură să demonstreze că prelucrarea este efectuată în conformitate cu RGPD, în special cu principiile fundamentale de protecție a datelor prevăzute la articolul 5 alineatul (1). Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice și trebuie să fie revizuite și actualizate atunci când este necesar⁴².

6.5 Crearea de profiluri

81. Prelucrarea datelor cu caracter personal de către prestatorii de servicii de plată poate implica „crearea de profiluri”, astfel cum se menționează la articolul 4 alineatul (4) din RGPD. De exemplu, PSIC s-ar putea baza pe prelucrarea automată a datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică. Situația financiară personală a unei persoane vizate ar putea fi evaluată în funcție de caracteristicile serviciului. Serviciile de informare cu privire la conturi, care urmează să fie furnizate conform solicitării utilizatorilor, pot implica o evaluare aprofundată a datelor personale privind conturile de plăți.
82. Operatorul trebuie, de asemenea, să fie transparent față de persoana vizată în ceea ce privește existența unui proces decizional automatizat, inclusiv crearea de profiluri. În aceste cazuri, operatorul trebuie să furnizeze informații relevante cu privire la logica utilizată, precum și cu privire la importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată [articolul 13 alineatul (2) litera (f), articolul 14 alineatul (2) litera (g) și considerentul 60]⁴³. De

³⁹ În conformitate cu Orientările Grupului de lucru „Articolul 29” privind transparența în temeiul Regulamentului 2016/679 – aprobate de CEPD, panourile privind confidențialitatea sunt deosebit de utile atunci când același serviciu este utilizat de persoanele vizate pe mai multe dispozitive diferite, deoarece le oferă acestora acces la datele lor cu caracter personal și controlul asupra acestora, indiferent de modul în care utilizează serviciul. Faptul că se permite persoanelor vizate să își ajusteze manual setările de confidențialitate prin intermediul unui panou de confidențialitate poate facilita, de asemenea, personalizarea unei declarații/unui anunț de confidențialitate prin faptul că se pot reflecta doar tipurile de prelucrare care se realizează pentru respectiva persoană vizată.

⁴⁰ A se vedea, de exemplu, „consimțământul explicit” menționat la articolul 67 alineatul (2) litera (a) din DSP2.

⁴¹ A se vedea, de asemenea, EBA/OP/2020/10, punctul 45.

⁴² Articolul 5 alineatul (2) și articolul 24 din RGPD.

⁴³ Orientări privind transparența în temeiul Regulamentului 2016/679, WP 260 rev.01 – aprobate de CEPD.

asemenea, în temeiul articolului 15 din RGPD, persoana vizată are dreptul de a solicita și de a obține informații de la operator cu privire la existența unui proces decizional automatizat, inclusiv la crearea de profiluri, logica implicată și consecințele pentru persoana vizată și, în anumite circumstanțe, dreptul de a se opune creării de profiluri, indiferent dacă are loc doar un proces decizional individual automatizat bazat pe crearea de profiluri⁴⁴.

83. În plus, ceea ce este relevant și în acest context este dreptul persoanei vizate de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice ce o privesc sau care o afectează în mod similar și semnificativ, prevăzută la articolul 22 din RGPD. În anumite circumstanțe, această normă include și necesitatea ca operatorii de date să pună în aplicare măsuri adecvate pentru a proteja drepturile persoanei vizate, cum ar fi informații specifice pentru persoana vizată, dreptul de a obține intervenție umană în procesul decizional și de a-și exprima punctul de vedere și de a contesta decizia. Astfel cum se menționează și în considerentul 71 din RGPD, aceasta înseamnă, printre altele, că persoanele vizate au dreptul de a nu face obiectul unei decizii, cum ar fi refuzul automat al unei cereri de credit online fără intervenție umană⁴⁵.
84. Procesul decizional automatizat, inclusiv crearea de profiluri care implică categorii speciale de date cu caracter personal, este permis numai în condițiile cumulative prevăzute la articolul 22 alineatul (4) din RGPD:
- există o derogare aplicabilă în temeiul articolului 22 alineatul (2);
 - și se aplică articolul 9 alineatul (2) litera (a) sau (g) din RGPD. În ambele cazuri, operatorul instituie măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate⁴⁶.
85. Cerințele privind prelucrarea ulterioară, astfel cum sunt prevăzute în prezentele orientări, ar trebui, de asemenea, să fie respectate. Clarificările și instrucțiunile privind procesul decizional individual automatizat și crearea de profiluri emise de Grupul de lucru „Articolul 29” privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679, astfel cum au fost aprobate de CEPD, sunt pe deplin relevante în contextul serviciilor de plată și, prin urmare, ar trebui luate în considerare în mod corespunzător.

Pentru Comitetul european pentru protecția datelor,

Președintele

(Andrea Jelinek)

⁴⁴ Orientările Grupului de lucru „Articolul 29” privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP251 rev.01.

⁴⁵ Considerentul 71 din RGPD.

⁴⁶ Orientările Grupului de lucru „Articolul 29” privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679, WP251 rev.01, pagina 24.