Smjernice 6/2020 o međudjelovanju Druge direktive o platnim uslugama i Opće uredbe o zaštiti podataka (GDPR)

Verzija 2.0

Donesene 15. prosinca 2020.

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

Povijest verzija

Verzija 2.0	15. 12. 2020.	Donošenje Smjernica nakon javnog savjetovanja
Verzija 1.0	17. 7. 2020.	Donošenje Smjernica za javno savjetovanje

Sadržaj

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „GDPR"),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru (EGP), posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članke 12. i 22. svojeg poslovnika,

budući da:

(1) GDPR-om se predviđa dosljedan skup pravila za obradu osobnih podataka diljem EU-a.

(2) Drugom direktivom o platnim uslugama (Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 23. prosinca 2015.) stavlja se izvan snage Direktiva 2007/64/EZ i predviđaju se nova pravila kako bi se osigurala pravna sigurnost za potrošače, trgovce i trgovačka društva u lancu plaćanja te modernizirao pravni okvir za tržište platnih usluga[2]. Države članice morale su prenijeti Drugu direktivu o platnim uslugama u svoje nacionalno pravo prije 13. siječnja 2018.

(3) Važna je značajka Druge direktive o platnim uslugama uvođenje pravnog okvira za nove usluge iniciranja plaćanja i usluge pružanja informacija o računu. Drugom direktivom o platnim uslugama tim se novim pružateljima platnih usluga omogućuje pristup računima za plaćanje ispitanika u svrhu pružanja navedenih usluga.

(4) U vezi sa zaštitom podataka, u skladu s člankom 94. stavkom 1. Druge direktive o platnim uslugama, svaka obrada osobnih podataka, uključujući pružanje informacija o obradi, za potrebe Druge direktive o platnim uslugama provodi se u skladu s GDPR-om[3] i Uredbom (EU) 2018/1725.

(5) U uvodnoj izjavi 89. Druge direktive o platnim uslugama navodi se sljedeće: ako se osobni podaci obrađuju za potrebe Druge direktive o platnim uslugama, trebalo bi navesti točnu svrhu obrade, primjenjivu pravnu osnovu, provesti relevantne sigurnosne zahtjeve utvrđene u GDPR-u te poštovati načela nužnosti, razmjernosti, ograničenja svrhe i razmjernog razdoblja zadržavanja podataka. Osim toga, tehnička i integrirana zaštita podataka trebala bi se ugraditi u sve sustave za obradu podataka koji se razvijaju i upotrebljavaju u okviru Druge direktive o platnim uslugama[4].

(6) U uvodnoj izjavi 93. Druge direktive o platnim uslugama navodi se da bi pružatelji usluga iniciranja plaćanja i pružatelji usluga pružanja informacija o računu, s jedne strane, i pružatelj platnih usluga koji vodi račun, s druge strane, trebali poštovati potrebne zahtjeve za zaštitu podataka i sigurnosne zahtjeve koji su utvrđeni tom direktivom ili navedeni u njoj ili su uključeni u regulatorne tehničke standarde.

[1]Upućivanja na „države članice" u ovom dokumentu trebaju se tumačiti kao upućivanja na „države članice EGP-a".
[2] Uvodna izjava 6. Druge direktive o platnim uslugama.
[3] Budući da Druga direktiva o platnim uslugama prethodi GDPR-u, ona i dalje upućuje na Direktivu 95/46. U članku 94. GDPR-a navodi se da se upućivanja na Direktivu 95/46, koja je stavljena izvan snage, tumače kao upućivanja na GDPR.
[4] Uvodna izjava 89., Druga direktiva o platnim uslugama.

DONIO JE SLJEDEĆE SMJERNICE:

1. UVOD

1. Drugom direktivom o platnim uslugama uveden je niz novina u području platnih usluga. Iako se njome stvaraju nove prilike za potrošače i povećava transparentnost u tom području, zbog primjene Druge direktive o platnim uslugama pojavljuju se određena pitanja i dvojbe u pogledu potrebe da ispitanici i dalje imaju potpunu kontrolu nad svojim osobnim podacima. GDPR se primjenjuje na obradu osobnih podataka, uključujući aktivnosti obrade koje se provode u kontekstu platnih usluga kako su definirane Drugom direktivom o platnim uslugama[5]. Stoga voditelji obrade koji djeluju u području obuhvaćenom Drugom direktivom o platnim uslugama uvijek moraju osigurati usklađenost sa zahtjevima GDPR-a, uključujući načela zaštite podataka iz članka 5. GDPR-a, kao i relevantne odredbe Direktive o e-privatnosti[6]. Dok Druga direktiva o platnim uslugama[7] i regulatorni tehnički standardi za pouzdanu autentifikaciju klijenta te zajedničke i sigurne otvorene standarde komunikacije (dalje u tekstu „RTS")[8] sadržavaju određene odredbe koje se odnose na zaštitu i sigurnost podataka, pojavila se nesigurnost u pogledu tumačenja tih odredaba te međudjelovanja općeg okvira za zaštitu podataka i Druge direktive o platnim uslugama.

2. Europski odbor za zaštitu podataka (EDPB) izdao je 5. srpnja 2018. dopis u vezi s Drugom direktivom o platnim uslugama, u kojem je pojasnio pitanja koja se odnose na zaštitu osobnih podataka u vezi s Drugom direktivom o platnim uslugama, posebno u pogledu obrade osobnih podataka neugovornih stranaka (takozvani „podaci tihe strane") koju provode pružatelji usluga pružanja informacija o računu (dalje u tekstu „AISP-i") i pružatelji usluga iniciranja plaćanja (dalje u tekstu „PISP-i"), postupaka u vezi s davanjem i povlačenjem suglasnosti, regulatornih tehničkih standarda i suradnje između pružatelja platnih usluga koji vode račune (dalje u tekstu „ASPSP-i") u odnosu na sigurnosne mjere. Pripremni rad na ovim Smjernicama obuhvaćao je prikupljanje doprinosa dionika, i u pisanom obliku i na događaju za dionike, kako bi se utvrdili najhitniji izazovi.

3. Cilj je ovih Smjernica pružiti dodatne upute o aspektima zaštite podataka u kontekstu Druge direktive o platnim uslugama, posebno u pogledu odnosa između relevantnih odredaba GDPR-a i Druge direktive o platnim uslugama. Glavni je naglasak ovih Smjernica na obradi osobnih podataka koju provode AISP-i i PISP-i. Dokument se kao takav bavi uvjetima za odobrenje pristupa informacijama o računima za plaćanje koje daju ASPSP-i i za obradu osobnih podataka koju provode PISP-i i AISP-i, uključujući zahtjeve i zaštitu u vezi s obradom osobnih podataka koju provode PISP-i i AISP-i u svrhe koje nisu prvotne svrhe za koje su podaci prikupljeni, posebno ako

[5] Članak 1. stavak 1. GDPR-a.
[6] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama); SL L 201, 31.7.2002., str. 37.–47.
[7] Članak 94. Direktive o platnim uslugama itd.
[8] Delegirana uredba Komisije (EU) 2018/389 od 27. studenoga 2017. o dopuni Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda za pouzdanu autentifikaciju klijenta i zajedničke i sigurne otvorene standarde komunikacije (tekst značajan za EGP); C/2017/7782; SL L 69, 13.3.2018., str. 23.–43.; dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32018R0389&from=HR

su prikupljeni u kontekstu pružanja usluge pružanja informacija o računu[9]. Dokument se bavi i različitim poimanjima izričite privole odnosno suglasnosti sadržanima u Drugoj direktivi o platnim uslugama i GDPR-u, obradom „podataka tihe strane", obradom posebnih kategorija osobnih podataka koju provode PISP-i i AISP-i te primjenom glavnih načela zaštite podataka utvrđenih GDPR-om, uključujući smanjenje količine podataka, transparentnost, odgovornost i sigurnosne mjere. Druga direktiva o platnim uslugama uključuje transverzalne odgovornosti u područjima, među ostalim, zaštite potrošača i prava tržišnog natjecanja. Razmatranja u pogledu tih područja prava izvan su područja primjene ovih Smjernica.

4. Kako bi se olakšalo čitanje smjernica, u nastavku se navode glavne definicije koje se upotrebljavaju u ovom dokumentu.

1.1. Definicije

„Pružatelj usluga pružanja informacija o računu" („AISP") odnosi se na pružatelja internetske usluge pružanja konsolidiranih informacija o jednom ili više računa za plaćanje koje korisnik platnih usluga ima kod drugog pružatelja platnih usluga ili kod više pružatelja platnih usluga.

„Pružatelj platnih usluga koji vodi račun" („ASPSP") odnosi se na pružatelja platnih usluga koji platitelju pruža i održava račun za plaćanje.

„Smanjenje količine podataka" načelo je zaštite podataka prema kojem su osobni podaci primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.

„Platitelj" se odnosi na fizičku ili pravnu osobu koja ima račun za plaćanje i koja daje suglasnost za izvršenje naloga za plaćanje s tog računa za plaćanje ili, ako račun za plaćanje ne postoji, fizička ili pravna osoba koja daje nalog za plaćanje.

„Primatelj plaćanja" odnosi se na fizičku ili pravnu osobu koja je predviđeni primatelj novčanih sredstava koja su predmet platne transakcije.

„Račun za plaćanje" znači račun koji se vodi u ime jednog ili više korisnika platnih usluga i koji se koristi za izvršenje platnih transakcija.

„Pružatelj usluge iniciranja plaćanja" („PISP") odnosi se na pružatelja usluge iniciranja naloga za plaćanje na zahtjev korisnika platne usluge u vezi s računom za plaćanje koji vodi drugi pružatelj platnih usluga.

„Pružatelj platnih usluga" odnosi se na tijelo iz članka 1. stavka 1. Druge direktive o platnim uslugama[10] ili na fizičku ili pravnu osobu kojoj je dopušteno izuzeće na temelju članka 32. ili 33. Druge direktive o platnim uslugama.

[9] Usluga pružanja informacija o računu internetska je usluga pružanja konsolidiranih informacija o jednom ili više računa za plaćanje koje korisnik platnih usluga ima kod drugog pružatelja platnih usluga ili kod više pružatelja platnih usluga.

[10] U članku 1. stavku 1. Druge direktive o platnim uslugama navodi se da se Drugom direktivom o platnim uslugama utvrđuju pravila u skladu s kojima države članice razlikuju sljedeće kategorije pružatelja platnih usluga:
(a) kreditne institucije kako su definirane člankom 4. stavkom 1. točkom 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća (1), uključujući njihove podružnice u smislu članka 4. stavka 1. točke 17. te uredbe kada se te podružnice nalaze u Uniji, bez obzira na to nalaze li se sjedišta tih podružnica unutar Unije ili, u skladu s člankom 47. Direktive 2013/36/EU i nacionalnim pravom, izvan Unije

„Korisnik platnih usluga” znači fizička ili pravna osoba koja koristi platnu uslugu u svojstvu platitelja, primatelja plaćanja, ili jednog i drugog.

„Osobni podaci” znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

„Tehnička zaštita podataka” odnosi se na tehničke i organizacijske mjere ugrađene u proizvod ili uslugu, koje su osmišljene za učinkovitu provedbu načela zaštite podataka i integriranja potrebne zaštite u obradu kako bi se ispunili zahtjevi GDPR-a i zaštitila prava ispitanika.

„Integrirana zaštita podataka” odnosi se na odgovarajuće tehničke i organizacijske mjere koje se provode kod proizvoda ili usluge i kojima se osigurava da se automatski obrađuju samo osobni podaci koji su potrebni za svaku posebnu svrhu obrade.

„RTS” se odnosi na Delegiranu uredbu Komisije (EU) 2018/389 od 27. studenoga 2017. o dopuni Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda za pouzdanu autentifikaciju klijenta i zajedničke i sigurne otvorene standarde komunikacije.

„Treće strane koje su pružatelji usluga” odnose se na PISP-e i AISP-e.

1.2. Usluge u skladu s Drugom direktivom o platnim uslugama

5. Drugom direktivom o platnim uslugama uvode se dvije nove vrste platnih usluga (pružatelja usluga): PISP-i i AISP-i. Prilog 1. Drugoj direktivi o platnim uslugama sadržava osam platnih usluga koje su obuhvaćene Drugom direktivom o platnim uslugama.

6. PISP-i pružaju usluge iniciranja naloga za plaćanje na zahtjev korisnika platnih usluga u vezi s korisnikovim računom za plaćanje kod drugog pružatelja platnih usluga[11]. PISP može od ASPSP-a (obično banke) zatražiti iniciranje transakcije u ime korisnika platnih usluga. Korisnik (platne usluge) može biti fizička osoba (ispitanik) ili pravna osoba.

7. AISP-i pružaju internetske usluge konsolidiranih informacija o jednom ili više računa za plaćanje koje korisnik platnih usluga ima kod drugog pružatelja platnih usluga ili kod više pružatelja platnih usluga[12]. U skladu s uvodnom izjavom 28. Druge direktive o platnim uslugama, korisnik platnih usluga može odmah u bilo kojem trenutku imati cjelovit uvid u svoju financijsku situaciju.

8. Kad je riječ o uslugama pružanja informacija o računu, moglo bi se ponuditi nekoliko različitih vrsta usluga, s naglaskom na različitim značajkama i svrhama. Na primjer, neki pružatelji usluga mogu korisnicima ponuditi usluge kao što su planiranje proračuna i praćenje potrošnje. Obrada osobnih

(b) institucije za elektronički novac u smislu članka 2. točke 1. Direktive 2009/110/EZ, uključujući, u skladu s člankom 8. te direktive i nacionalnim pravom, njihove podružnice kada se te podružnice nalaze u Uniji, a njihova se sjedišta nalaze izvan Unije, u mjeri u kojoj su platne usluge koje te podružnice pružaju povezane s izdavanjem elektroničkog novca
(c) poštanske žiro-institucije koje u skladu s nacionalnim pravom imaju pravo pružati platne usluge
(d) institucije za platni promet
(e) Europska središnja banka (ESB) i nacionalne središnje banke kada ne djeluju u svojstvu monetarnog tijela ili drugog tijela javne vlasti
(f) države članice ili njihove jedinice regionalne ili lokalne uprave kada ne djeluju u svojstvu tijela javne vlasti.

[11] Članak 4. stavak 15. Druge direktive o platnim uslugama.

[12] Članak 4. stavak 16. Druge direktive o platnim uslugama.

podataka u kontekstu tih usluga obuhvaćena je Drugom direktivom o platnim uslugama. Usluge koje uključuju procjene kreditne sposobnosti korisnika platnih usluga ili usluge revizije koje se provode na temelju prikupljanja informacija uslugom pružanja informacija o računu nisu obuhvaćene područjem primjene Druge direktive o platnim uslugama i stoga su obuhvaćene GDPR-om. Nadalje, Drugom direktivom o platnim uslugama nisu obuhvaćeni ni računi koji nisu računi za plaćanje (npr. štedni ili investicijski računi). U svakom slučaju, GDPR je primjenjivi pravni okvir za obradu osobnih podataka.

Primjer 1.:

HappyPayments je društvo koje nudi internetsku uslugu koja se sastoji od pružanja informacija o jednom računu za plaćanje ili više njih s pomoću mobilne aplikacije kako bi se osigurao financijski nadzor (usluga pružanja informacija o računu). S pomoću ove usluge korisnik platnih usluga može na jednome mjestu vidjeti salda i nedavne transakcije na dvama računima ili više računa za plaćanje u različitim bankama. Kada korisnik platnih usluga tako odluči, u okviru usluge nudi se i kategorizacija troškova i prihoda prema različitim tipologijama (plaća, slobodno vrijeme, energija, hipoteka itd.), čime se korisniku platnih usluga pomaže u financijskom planiranju. U okviru te aplikacije HappyPayments nudi i uslugu za iniciranje plaćanja izravno s korisnikovih računa određenih za plaćanje (usluga iniciranja plaćanja).

9. Kako bi se pružile te usluge, Drugom direktivom o platnim uslugama uređuju se pravni uvjeti pod kojima PISP-i i AISP-i mogu pristupiti računima za plaćanje kako bi korisniku platnih usluga pružili uslugu.

10. Člankom 66. stavkom 1. i člankom 67. stavkom 1. Druge direktive o platnim uslugama utvrđuje se da su korištenje platnih usluga i usluga pružanja informacija o računu te pristup tim uslugama prava korisnika platnih usluga. To znači da bi korisnik platnih usluga trebao ostati potpuno slobodan u pogledu ostvarivanja tog prava i ne može ga se prisiliti da iskoristi to pravo.

11. Pristup računima za plaćanje i upotreba informacija o računu za plaćanje djelomično su uređeni člancima 66. i 67. Druge direktive o platnim uslugama, koji sadržavaju zaštitne mjere u pogledu zaštite (osobnih) podataka. U članku 66. stavku 3. točki (f) Druge direktive o platnim uslugama navodi se da PISP ne smije od korisnika platnih usluga tražiti bilo koje druge podatke osim onih koji su potrebni za pružanje usluge iniciranja plaćanja, a člankom 66. stavkom 3. točkom (g) Druge direktive o platnim uslugama propisuje se da PISP-i ne smiju upotrebljavati podatke, pristupati im ili ih pohranjivati u bilo koju drugu svrhu osim pružanja usluge iniciranja plaćanja kako je platitelj izričito zatražio. Nadalje, člankom 67. stavkom 2. točkom (d) Druge direktive o platnim uslugama pristup koji imaju AISP-i ograničava se na informacije s utvrđenih računa za plaćanje i s njima povezane platne transakcije, dok se u članku 67. stavku 2. točki (f) Druge direktive o platnim uslugama navodi da AISP-i ne smiju upotrebljavati podatke, pristupati im niti ih pohranjivati u bilo koju drugu svrhu osim obavljanja usluge pružanja informacija o računu koju je korisnik platnih usluga izričito zatražio, u skladu s pravilima o zaštiti podataka. U potonjem se naglašava da se, u okviru usluga pružanja informacija o računu, osobni podaci mogu prikupljati samo u određene, izričite i zakonite svrhe. Stoga bi AISP u ugovoru trebao izričito navesti u koje će se određene svrhe osobni podaci povezani s informacijama o računu obrađivati u kontekstu usluge pružanja informacija o računu. Ugovor bi trebao biti zakonit, pošten i transparentan u skladu s člankom 5. GDPR-a, kao i sukladan drugim zakonima o zaštiti potrošača.

12. Ovisno o određenim okolnostima, pružatelji platnih usluga mogu biti voditelji obrade podataka ili izvršitelji obrade podataka u skladu s GDPR-om. U ovim Smjernicama „voditelji obrade” pružatelji su platnih usluga koji sami ili zajedno s drugima određuju svrhe i načine obrade osobnih podataka.

Više informacija o tome nalazi se u Smjernicama EDPB-a 7/2020 o pojmovima voditelja i izvršitelja obrade u Općoj uredbi o zaštiti podataka (GDPR).

2. ZAKONITA OSNOVA I DALJNJA OBRADA NA TEMELJU DRUGE DIREKTIVE O PLATNIM USLUGAMA

2.1. Zakonita osnova za obradu

13. U skladu s GDPR-om voditelji obrade moraju imati pravnu osnovu za obradu osobnih podataka. Članak 6. stavak 1. GDPR-a iscrpan je i ograničavajući popis šest pravnih osnova za obradu osobnih podataka u skladu s GDPR-om[13]. Voditelj obrade mora definirati odgovarajuću pravnu osnovu i uvjeriti se da su ispunjeni svi uvjeti za tu pravnu osnovu. Odluka o tome koja je osnova u određenoj situaciji valjana i najprikladnija ovisi o okolnostima u kojima se obrada odvija, uključujući svrhu obrade i odnos između voditelja obrade i ispitanika.

2.2. Članak 6. stavak 1. točka (b) GDPR-a (obrada je nužna za izvršavanje ugovora)

14. Platne usluge pružaju se na ugovornoj osnovi između korisnika platnih usluga i pružatelja platnih usluga. Kako je navedeno u uvodnoj izjavi 87. Druge direktive o platnim uslugama, „[p]redmet ove Direktive trebale bi biti samo ugovorne obveze i odgovornosti između korisnika platnih usluga i pružatelja platnih usluga.” U smislu GDPR-a, glavna je pravna osnova za obradu osobnih podataka radi pružanja platnih usluga članak 6. stavak 1. točka (b) GDPR-a, što znači da je obrada nužna za izvršenje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora.

15. Platne usluge u skladu s Drugom direktivom o platnim uslugama definirane su u Prilogu 1. Drugoj direktivi o platnim uslugama. Pružanje tih usluga kako je definirano Drugom direktivom o platnim uslugama preduvjet je za sklapanje ugovora u kojem stranke imaju pristup podacima o računu za plaćanje korisnika platnih usluga. Ti pružatelji platnih usluga moraju biti i ovlašteni operateri. U odnosu na usluge iniciranja plaćanja i usluge pružanja informacija o računu u skladu s Drugom direktivom o platnim uslugama, ugovori mogu sadržavati uvjete kojima se nameću i uvjeti za dodatne usluge koje nisu uređene Drugom direktivom o platnim uslugama. U Smjernicama EDPB-a 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima jasno se navodi da voditelji obrade moraju procijeniti koja je obrada osobnih podataka objektivno nužna za izvršenje ugovora. U tim se smjernicama ističe da opravdanje nužnosti ovisi o prirodi usluge, zajedničkim perspektivama i očekivanjima ugovornih stranaka, obrazloženju ugovora i njegovim osnovnim elementima.

[13] U skladu s člankom 6. obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

(a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha

(b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora

(c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade

(d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe

(e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade

(f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

16. U Smjernicama EDPB-a 2/2019 pojašnjava se i da se, s obzirom na članak 7. stavak 4. GDPR-a, razlikuju aktivnosti obrade nužne za izvršenje ugovora i odredbe koje uslugu uvjetuju određenim aktivnostima obrade koje zapravo nisu nužne za izvršenje ugovora. Formulacijom „nužne za izvršenje" jasno se zahtijeva nešto više od ugovornog uvjeta[14]. Voditelj obrade trebao bi moći dokazati kako se glavni predmet određenog ugovora s ispitanikom ne može zapravo izvršiti ako se ne obavi određena obrada predmetnih podataka. Samo upućivanje na obradu ili navođenje obrade podataka u ugovoru nije dovoljno da bi se predmetna obrada obuhvatila područjem primjene članka 6. stavka 1. točke (b) GDPR-a.

17. Člankom 5. stavkom 1. točkom (b) GDPR-a predviđeno je načelo ograničenja svrhe, kojim se zahtijeva da se osobni podaci moraju prikupljati u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Pri procjeni je li članak 6. stavak 1. točka (b) odgovarajuća pravna osnova za internetsku (platnu) uslugu, trebalo bi uzeti u obzir konkretnu svrhu, namjenu ili cilj usluge[15]. Svrhe obrade moraju biti jasno navedene i priopćene ispitaniku, u skladu s ograničenjem svrhe voditelja obrade i obvezama u pogledu transparentnosti. Procjena onoga što je „nužno" obuhvaća kombiniranu procjenu obrade temeljenu na činjenicama „za cilj kojem se teži i je li to manje nametljivo u odnosu na druge mogućnosti za postizanje istog cilja". Člankom 6. stavkom 1. točkom (b) nije obuhvaćena obrada koja je korisna, ali nije objektivno nužna za izvršenje ugovorne usluge ili za poduzimanje odgovarajućih predugovornih koraka na zahtjev ispitanika, čak i ako je to nužno za ostale poslovne svrhe voditelja obrade[16].

18. U Smjernicama EDPB-a 2/2019 pojašnjava se da se ugovorima ne mogu umjetno proširiti kategorije osobnih podataka ili vrsta aktivnosti obrade koje voditelj obrade mora provesti radi izvršenja ugovora u okviru značenja članka 6. stavka 1. točke (b)[17]. Te se smjernice bave i slučajevima u kojima se ispitanike koji su možda zainteresirani samo za jednu od usluga dovodi u situacije tipa „uzmi ili ostavi". To se može dogoditi kada voditelj obrade želi spojiti nekoliko pojedinačnih usluga ili elemenata usluge s različitim osnovnim svrhama, značajkama ili obrazloženjima u jedan ugovor. Ako se ugovor sastoji od nekoliko pojedinačnih usluga ili elemenata usluge koji zaista mogu biti razumno provedeni neovisno jedan o drugom, primjenjivost članka 6. stavka 1. točke (b) trebala bi se procjenjivati u kontekstu svake od tih usluga pojedinačno, gledajući ono što je objektivno nužno za izvršavanje svake pojedinačne usluge koju je ispitanik aktivno zatražio ili za koju se prijavio[18].

19. U skladu s prethodno navedenim smjernicama, voditelji obrade moraju procijeniti što je objektivno nužno za izvršenje ugovora. Ako voditelji obrade ne mogu dokazati da je obrada osobnih podataka o računu za plaćanje objektivno nužna za pružanje svake od tih usluga zasebno, članak 6. stavak 1. točka (b) GDPR-a nije valjana pravna osnova za obradu. U tim bi slučajevima voditelj obrade trebao razmotriti drugu pravnu osnovu za obradu.

2.3. Sprječavanje prijevara

20. U članku 94. stavku 1. Druge direktive o platnim uslugama navodi se da države članice dopuštaju obradu osobnih podataka u platnim sustavima te pružateljima platnih usluga kada je to potrebno za zaštitu sprječavanja, istraživanja i otkrivanja prijevara u platnom prometu. Obrada osobnih podataka koja je strogo nužna u svrhu sprječavanja prijevare mogla bi predstavljati legitiman

[14] Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima, EDPB, stranica 8.
[15] Isto.
[16] Isto, stranica 7.
[17] Isto, stranica 10.
[18] Isto, stranica 11.

interes dotičnog pružatelja platnih usluga, pod uvjetom da takvi interesi nisu podređeni interesima ili temeljnim pravima i slobodama ispitanika[19]. Aktivnosti obrade u svrhu sprječavanja prijevara trebale bi se temeljiti na pažljivoj pojedinačnoj procjeni koju provodi voditelj obrade, u skladu s načelom odgovornosti. Osim toga, kako bi se spriječile prijevare, voditelji obrade mogu podlijegati i posebnim pravnim obvezama koje zahtijevaju obradu osobnih podataka.

2.4. Daljnja obrada (AISP i PISP)

21. Člankom 6. stavkom 4. GDPR-a utvrđuju se uvjeti za obradu osobnih podataka u svrhu različitu od one za koju su osobni podaci prikupljeni. Konkretnije, takva daljnja obrada može se odvijati ako se temelji na pravu Unije ili države članice koje predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu ciljeva iz članka 23. stavka 1. ako je ispitanik dao svoju privolu ili ako je obrada u svrhu različitu od one za koju su osobni podaci prikupljeni u skladu s prvotnom svrhom.

22. Članak 66. stavak 3. točku (g) i članak 67. stavak 2. točku (f) Druge direktive o platnim uslugama treba pažljivo razmotriti. Kako je prethodno navedeno, u članku 66. stavku 3. točki (g) Druge direktive o platnim uslugama navodi se da PISP ne smije upotrebljavati podatke, pristupati im ili ih pohranjivati u bilo koju drugu svrhu osim pružanja usluge iniciranja plaćanja kako je platitelj izričito zatražio. U članku 67. stavku 2. točki (f) Druge direktive o platnim uslugama navodi se da AISP ne upotrebljava podatke, ne pristupa im niti ih pohranjuje u bilo koju drugu svrhu osim obavljanja usluge pružanja informacija o računu koju je korisnik platnih usluga izričito zatražio, u skladu s pravilima o zaštiti podataka.

23. Stoga se člankom 66. stavkom 3. točkom (g) i člankom 67. stavkom 2. točkom (f) Druge direktive o platnim uslugama znatno ograničavaju mogućnosti obrade u druge svrhe, što znači da obrada u drugu svrhu nije dopuštena, osim ako je ispitanik dao privolu u skladu s člankom 6. stavkom 1. točkom (a) GDPR-a ili ako je obrada propisana pravom Unije ili pravom države članice kojem voditelj obrade podliježe, u skladu s člankom 6. stavkom 4. GDPR-a. Ako se obrada u svrhu različitu od one za koju su osobni podaci prikupljeni ne temelji na privoli ispitanika ili na pravu Unije ili države članice, ograničenjima utvrđenima u članku 66. stavku 3. točki (g) i članku 67. stavku 2. točki (f) Druge direktive o platnim uslugama jasno se utvrđuje da bilo koja druga svrha nije u skladu sa svrhom u koju se osobni podaci prvotno prikupljaju. Test kompatibilnosti iz članka 6. stavka 4. GDPR-a ne može dovesti do pravne osnove za obradu.

24. Člankom 6. stavkom 4. GDPR-a omogućuje se daljnja obrada na temelju prava Unije ili prava države članice. Na primjer, svi su PISP-i i AISP-i obveznici u skladu s člankom 3. stavkom 2. točkom (a) Direktive (EU) 2015/849 Europskog parlamenta i Vijeća od 20. svibnja 2015. o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma iz Direktive o borbi protiv pranja novca. Stoga su ti obveznici obvezni primijeniti mjere dubinske analize stranke kako je navedeno u Direktivi. Stoga se osobni podaci koji se obrađuju u vezi s uslugom iz Druge direktive o platnim uslugama dalje obrađuju na temelju barem jedne pravne obveze pružatelja usluga[20].

25. Kako je navedeno u točki 20., u članku 6. stavku 4. GDPR-a navodi se da bi se obrada u svrhu različitu od svrhe u koju su osobni podaci prikupljeni mogla temeljiti na privoli ispitanika ako su ispunjeni svi uvjeti za privolu iz GDPR-a. Kako je prethodno navedeno, voditelj obrade mora dokazati da je privolu moguće odbiti ili povući bez posljedica (uvodna izjava 42. GDPR-a).

2.5. Zakonita osnova za odobravanje pristupa računu (ASPSP-i)

[19] Uvodna izjava 47. GDPR-a.

[20] Treba napomenuti da temeljito ispitivanje usklađenosti Direktive o borbi protiv pranja novca sa standardom iz članka 6. stavka 4. GDPR-a nije obuhvaćeno područjem primjene ovog dokumenta.

26. Kako je navedeno u točki 10., korisnici platnih usluga mogu ostvariti svoje pravo na korištenje usluga iniciranja plaćanja i usluga pružanja informacija o računu. Obveze propisane za države članice u članku 66. stavku 1. i članku 67. stavku 1. Druge direktive o platnim uslugama trebale bi se prenijeti u nacionalno pravo kako bi se zajamčila djelotvorna primjena prava korisnika platnih usluga na korištenje prethodno navedenih platnih usluga. Učinkovita primjena takvih prava ne bi bila moguća bez postojanja odgovarajuće obveze ASPSP-a, obično banke, da pružatelju platnih usluga odobri pristup računu pod uvjetom da je ispunio sve zahtjeve za pristup računu korisnika platnih usluga. Nadalje, u članku 66. stavku 5. i članku 67. stavku 4. Druge direktive o platnim uslugama jasno se navodi da pružanje usluga iniciranja plaćanja i usluga pružanja informacija o računu ne ovisi o postojanju ugovornog odnosa između PISP-a/AISP-a i ASPSP-a.

27. Obrada osobnih podataka koju provodi ASPSP i koja se sastoji od odobravanja pristupa osobnim podacima koji su zatražili PISP i AISP kako bi mogli izvršiti svoju platnu uslugu prema korisniku platnih usluga, temelji se na pravnoj obvezi. Kako bi se ostvarili ciljevi Druge direktive o platnim uslugama, ASPSP-i moraju pružati osobne podatke za usluge PISP-a i AISP-a, što je nužan uvjet kako bi PISP-i i AISP-i mogli pružati svoje usluge i tako osigurati prava predviđena člankom 66. stavkom 1. i člankom 67. stavkom 1. Druge direktive o platnim uslugama. Stoga je pravna osnova koja se u ovom slučaju primjenjuje članak 6. stavak 1. točka (c) GDPR-a.

28. Budući da je GDPR-om utvrđeno da bi obrada koja se temelji na pravnoj obvezi trebala biti jasno utvrđena pravom Unije ili pravom države članice (vidjeti članak 6. stavak 3. GDPR-a), obveza ASPSP-a da odobre pristup trebala bi proizlaziti iz nacionalnog prava u koje je prenesena Druga direktiva o platnim uslugama.

3. IZRIČITA PRIVOLA ODNOSNO SUGLASNOST

3.1. Privola u skladu s GDPR-om

29. Na temelju GDPR-a privola je jedna od šest pravnih osnova za zakonitost obrade osobnih podataka. U članku 4. stavku 11. GDPR-a privola se definira kao „svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose". Ta četiri uvjeta – dobrovoljnost, posebnost, informiranost i nedvosmislenost pristanka – ključna su za valjanost privole. U skladu sa Smjernicama EDPB-a 5/2020 o privoli na temelju Uredbe 2016/679, privola može biti primjerena zakonita osnova samo ako ispitanik ima nadzor i istinski izbor u pogledu prihvaćanja ponuđenih uvjeta ili njihova odbijanja bez štetnih posljedica. Pri traženju privole dužnost je voditelja obrade da procijeni hoće li biti ispunjeni svi zahtjevi za dobivanje valjane privole. Ako je dobivena u potpunoj sukladnosti s GDPR-om, privola je alat kojim se ispitanicima omogućuje da odluče o tome hoće li se njihovi osobni podaci obrađivati. Ako to nije slučaj, nadzor ispitanika postaje iluzoran, a privola će biti nevažeća pravna osnova za obradu, čime aktivnost obrade postaje nezakonita[21].

30. GDPR sadržava i dodatnu zaštitu u članku 7. u kojem se navodi da voditelj obrade podataka mora biti u mogućnosti dokazati da je u trenutku obrade postojala valjana privola. Osim toga, zahtjev za privolu mora se predočiti na način koji se jasno razlikuje od drugih pitanja, u razumljivom i lako dostupnom obliku, na jasnom i jednostavnom jeziku. Nadalje, ispitanika se mora obavijestiti o pravu na povlačenje privole u bilo kojem trenutku na jednako jednostavan način na koji je privolu i dao.

31. U skladu s člankom 9. GDPR-a privola je jedna od iznimaka od opće zabrane obrade posebnih kategorija osobnih podataka. Međutim, u tom slučaju privola ispitanika mora biti „izričita"[22].

32. U skladu sa Smjernicama EDPB-a 5/2020 o privoli na temelju Uredbe 2016/679, izričita privola na temelju GDPR-a odnosi se na ispitanikov način izražavanja privole. To znači da bi ispitanik trebao dati izričitu izjavu o privoli za posebnu svrhu (posebne svrhe) obrade. Izričita potvrda privole u pisanoj izjavi bila bi očigledan način da se osigura izričitost privole. Prema potrebi voditelj obrade može osigurati da ispitanik potpiše pisanu izjavu kako bi se uklonile sve moguće sumnje i mogući nedostatak dokaza u budućnosti.

33. Privola se ni u kojem slučaju ne može izvesti iz potencijalno dvosmislenih izjava ili radnji. Voditelj obrade mora biti svjestan i toga da se privola ne može dobiti istim prijedlogom kao pristajanje na ugovor ili prihvaćanje općih uvjeta usluge.

3.2. Suglasnost na temelju Druge direktive o platnim uslugama

34. EDPB napominje da je pravni okvir u pogledu izričite privole odnosno suglasnosti složen jer Druga direktiva o platnim uslugama i GDPR sadržavaju pojam „izričite suglasnosti" odnosno „izričite privole". To dovodi do pitanja treba li „izričitu suglasnost" kako je navedena u članku 94. stavku 2. Druge direktive o platnim uslugama tumačiti na isti način kao izričitu privolu iz GDPR-a.

3.2.1. Izričita suglasnost na temelju članka 94. stavka 2. Druge direktive o platnim uslugama

35. Druga direktiva o platnim uslugama sadržava niz posebnih pravila o obradi osobnih podataka, posebno u članku 94. stavku 1., kojim se utvrđuje da obrada osobnih podataka za potrebe Druge

[21] Smjernice 5/2020 o privoli na temelju Uredbe 2016/679, EDPB, točka 3.
[22] Vidjeti i Mišljenje 15/2011 o definiciji pristanka, WP187, str. 6.–8., i/ili Mišljenje 6/2014 o pojmu zakonitih interesa nadzornika podataka u skladu s člankom 7. Direktive 95/46/EZ (WP217), str. 9., 10., 13. i 14.

direktive o platnim uslugama mora biti u skladu s pravom EU-a o zaštiti podataka. Nadalje, člankom 94. stavkom 2. Druge direktive o platnim uslugama utvrđuje se da pružatelji platnih usluga smiju pristupiti osobnim podacima, obrađivati i zadržavati osobne podatke potrebne za pružanje platnih usluga samo uz izričitu suglasnost korisnika platnih usluga. U skladu s člankom 33. stavkom 2. Druge direktive o platnim uslugama, taj zahtjev izričite suglasnosti korisnika platnih usluga ne primjenjuje se na AISP-e. Međutim, člankom 67. stavkom 2. točkom (a) Druge direktive o platnim uslugama i dalje se predviđa izričita suglasnost AISP-a za pružanje usluge.

36. Kako je prethodno navedeno, popis zakonitih osnova za obradu u skladu s GDPR-om iscrpan je. Kako je navedeno u točki 14., pravna osnova za obradu osobnih podataka radi pružanja platnih usluga u načelu je članak 6. stavak 1. točka (b) GDPR-a, što znači da je obrada nužna za izvršenje ugovora u kojem je ispitanik stranka ili za poduzimanje koraka koje ispitanik zahtijeva prije sklapanja ugovora. Iz toga slijedi da se članak 94. stavak 2. Druge direktive o platnim uslugama ne može smatrati dodatnom pravnom osnovom za obradu osobnih podataka. S obzirom na prethodno navedeno, EDPB smatra da se ova točka treba tumačiti, s jedne strane, u skladu s primjenjivim pravnim okvirom za zaštitu podataka, a s druge strane tako da se sačuva njezin koristan učinak. Stoga bi izričitu suglasnost iz članka 94. stavka 2. Druge direktive o platnim uslugama trebalo smatrati dodatnim zahtjevom ugovorne prirode[23] u pogledu pristupa osobnim podacima te njihove naknadne obrade i pohrane u svrhu pružanja platnih usluga te ona zato nije jednaka (izričitoj) privoli iz GDPR-a.

37. „Izričita suglasnost" iz članka 94. stavka 2. Druge direktive o platnim uslugama ugovorna je suglasnost. To znači da bi članak 94. stavak 2. Druge direktive o platnim uslugama trebalo tumačiti na način da pri sklapanju ugovora s pružateljem platnih usluga u skladu s Drugom direktivom o platnim uslugama ispitanici moraju biti u potpunosti upoznati s određenim kategorijama osobnih podataka koji će se obrađivati. Nadalje, moraju biti upoznati s konkretnom svrhom (platne usluge) u koju će se njihovi osobni podaci obrađivati i moraju se izričito složiti s tim klauzulama. Takve bi se klauzule trebale jasno razlikovati od drugih pitanja kojima se bavi ugovor te bi ih ispitanik trebao izričito prihvatiti.

38. Ključni element pojma „izričita suglasnost" na temelju članka 94. stavka 2. Druge direktive o platnim uslugama stjecanje je pristupa osobnim podacima radi naknadne obrade i pohrane tih podataka u svrhu pružanja platnih usluga. To znači da pružatelj platnih usluga[24] još ne obrađuje osobne podatke, ali mu je potreban pristup osobnim podacima koji su obrađeni pod odgovornošću bilo kojeg drugog voditelja obrade. Ako korisnik platnih usluga sklopi ugovor s, primjerice, pružateljem usluga iniciranja plaćanja, taj pružatelj mora dobiti pristup osobnim podacima korisnika platnih usluga koji se obrađuju pod odgovornošću pružatelja platnih usluga koji vodi račun. Cilj je izričite suglasnosti iz članka 94. stavka 2. Druge direktive o platnim uslugama dopuštenje za dobivanje pristupa tim osobnim podacima, kako bi se moglo obrađivati i pohranjivati osobne podatke potrebne za pružanje platne usluge. Ako je ispitanik dao izričitu suglasnost, pružatelj platnih usluga koji vodi račun obvezan je omogućiti pristup navedenim osobnim podacima.

39. Iako suglasnost iz članka 94. stavka 2. Druge direktive o platnim uslugama nije pravna osnova za obradu osobnih podataka, ta se suglasnost konkretno odnosi na osobne podatke i zaštitu podataka te se njome korisniku platnih usluga osigurava transparentnost i određena razina kontrole[25]. Iako

[23] Dopis EDPB-a o Drugoj direktivi o platnim uslugama, 5. srpnja 2018., str. 4.
[24] To se odnosi na usluge od 1. do 7. iz Priloga 1. Drugoj direktivi o platnim uslugama.
[25] Članak 94. stavak 2. Druge direktive o platnim uslugama obuhvaćen je poglavljem 4. „Zaštita podataka".

se u Drugoj direktivi o platnim uslugama ne navode materijalni uvjeti za suglasnost iz njezina članka 94. stavka 2., trebalo bi je, kako je prethodno navedeno, tumačiti u skladu s primjenjivim pravnim okvirom za zaštitu podataka i na način kojim se čuva njegov koristan učinak.

40. U pogledu informacija koje trebaju dostaviti voditelji obrade i zahtjeva transparentnosti, u Smjernicama Radne skupine iz članka 29. o transparentnosti navodi se da je „središnji [...] aspekt načela transparentnosti, koji je prikazan u tim odredbama, to da bi ispitanici trebali moći unaprijed utvrditi opseg i posljedice obrade podataka i kasnije ne bi trebali biti iznenađeni načinima na koji su njihovi osobni podaci korišteni”[26].

41. Nadalje, kako se zahtijeva načelom ograničenja svrhe, osobni podaci moraju se prikupljati u posebne, izričite i zakonite svrhe (članak 5. stavak 1. točka (b) GDPR-a). Ako se osobni podaci prikupljaju u više od jedne svrhe „voditelji obrade trebali bi izbjegavati utvrđivanje samo jedne široke svrhe kako bi opravdali različite daljnje aktivnosti obrade koje su zapravo tek u maloj mjeri povezane sa stvarnom prvotnom svrhom”[27]. EDPB je nedavno, u kontekstu ugovora za internetske usluge, skrenuo pozornost na rizik od uključivanja općih uvjeta obrade u ugovore te je naveo da bi se svrha prikupljanja trebala jasno i posebno utvrditi: trebala bi biti dovoljno detaljna kako bi se utvrdilo koja vrsta obrade jest, a koja nije uključena u određenu svrhu, te kako bi se omogućilo da se usklađenost s pravom može ocijeniti, a mjere za zaštitu podataka primijeniti[28].

42. Kada se razmatra u kontekstu dodatnog zahtjeva izričite suglasnosti u skladu s člankom 94. stavkom 2. Druge direktive o platnim uslugama, to podrazumijeva da voditelji obrade moraju ispitanicima pružiti posebne i izričite informacije o posebnim svrhama koje je utvrdio voditelj obrade, u koje se njihovim osobnim podacima pristupa te u koje se oni obrađuju i zadržavaju. U skladu s člankom 94. stavkom 2. Druge direktive o platnim uslugama, ispitanici moraju izričito prihvatiti te posebne svrhe.

43. Osim toga, kao što je prethodno navedeno u točki 10., EDPB ističe da korisnik platnih usluga mora moći odabrati hoće li koristiti uslugu ili ne i da ga se na to ne može prisiljavati. Stoga i suglasnost u skladu s člankom 94. stavkom 2. Druge direktive o platnim uslugama mora biti dobrovoljna.

3.3. Zaključak

44. Izričita suglasnost iz Druge direktive o platnim uslugama razlikuje se od (izričite) privole iz GDPR-a. Izričita suglasnost iz članka 94. stavka 2. Druge direktive o platnim uslugama dodatni je zahtjev ugovorne prirode. Kad pružatelj platnih usluga treba pristup osobnim podacima radi pružanja platne usluge, potrebna je izričita suglasnost korisnika platnih usluga u skladu s člankom 94. stavkom 2. Druge direktive o platnim uslugama.

[26] Radna skupina iz članka 29., Smjernice o transparentnosti na temelju Uredbe 2016/679, točka 10. (donesene 11. travnja 2018.) – odobrio EDPB.
[27] Mišljenje 3/2013 Radne skupine iz članka 29. o ograničavanju svrhe (WP203), str. 16.
[28] Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima, točka 16. (verzija javnog savjetovanja) i Mišljenje 3/2013 Radne skupine iz članka 29. o ograničavanju svrhe (WP203), str. 15.–16.

4. OBRADA PODATAKA TIHIH STRANA

4.1. Podaci tihih strana

45. Pitanje zaštite podataka koje treba pažljivo razmotriti jest obrada takozvanih „podataka tihih strana”. U kontekstu ovog dokumenta podaci tihih strana osobni su podaci koji se odnose na ispitanika koji nije korisnik određenog pružatelja platnih usluga, ali čije osobne podatke taj određeni pružatelj platnih usluga obrađuje radi izvršenja ugovora između pružatelja i korisnika platnih usluga. To je, na primjer, slučaj kada korisnik platnih usluga, ispitanik A, koristi usluge nekog AISP-a, a ispitanik B proveo je niz platnih transakcija na račun za plaćanje ispitanika A. U tom se slučaju ispitanik B smatra „tihom stranom”, a osobni podaci (kao što su broj računa ispitanika B i novčani iznos koji je bio uključen u te transakcije) koji se odnose na ispitanika B smatraju se „podacima tihe strane”.

4.2. Legitimni interes voditelja obrade

46. Člankom 5. stavkom 1. točkom (b) GDPR-a zahtijeva se da se osobni podaci prikupljaju u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Nadalje, GDPR-om se propisuje da svaka obrada osobnih podataka mora biti nužna i razmjerna te u skladu s načelima zaštite podataka, kao što su načela ograničenja svrhe i smanjenja količine podataka.

47. GDPR-om se može omogućiti obrada podataka tihe strane ako je ta obrada nužna za potrebe legitimnih interesa voditelja obrade ili treće strane (članak 6. stavak 1. točka (f) GDPR-a). Međutim, takva obrada ne može se provoditi ako su od legitimnog interesa voditelja obrade „jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka”.

48. Zakonita osnova za obradu podataka tihe strane koju provode PISP-i i AISP-i, u kontekstu pružanja platnih usluga u skladu s Drugom direktivom o platnim uslugama, mogla bi stoga biti legitiman interes voditelja obrade ili treće strane za izvršenje ugovora s korisnikom platnih usluga. Potreba za obradom osobnih podataka tihe strane ograničena je i ovisi o razumnim očekivanjima tih ispitanika. U kontekstu pružanja platnih usluga obuhvaćenih Drugom direktivom o platnim uslugama potrebno je uspostaviti učinkovite i odgovarajuće mjere kako bi se osiguralo da interesi ili temeljna prava i slobode tihih strana ne budu nadvladani te da se poštuju razumna očekivanja tih ispitanika u pogledu obrade njihovih osobnih podataka. U tom pogledu voditelj obrade (AISP ili PISP) mora uspostaviti potrebne zaštitne mjere za obradu kako bi se zaštitila prava ispitanika. To uključuje tehničke mjere kojima se osigurava da se podaci tihe strane ne obrađuju u svrhu koja nije ona u koju su osobne podatke prvotno prikupili PISP-i i AISP-i. Ako je izvedivo, trebalo bi primijeniti i enkripciju ili druge tehnike kako bi se postigla odgovarajuća razina sigurnosti i smanjenja količine podataka.

4.3. Daljnja obrada osobnih podataka tihe strane

49. Kako je navedeno u točki 29., osobni podaci koji se obrađuju u vezi s platnom uslugom koja je uređena Drugom direktivom o platnim uslugama mogli bi se dalje obrađivati na temelju pravnih obveza pružatelja usluga. Te pravne obveze mogle bi se odnositi na osobne podatke tihe strane.

50. Kad je riječ o daljnjoj obradi podataka tihe strane na temelju legitimnog interesa, EDPB smatra da se ti podaci ne mogu upotrebljavati u drugu svrhu osim one za koju su prikupljeni, na temelju prava EU-a ili prava države članice. Privola tihe strane nije pravno izvediva jer bi se za njezino dobivanje morali prikupljati ili obrađivati osobni podaci tihe strane, za što se ne može pronaći pravna osnova na temelju članka 6. GDPR-a. Ni test usklađenosti iz članka 6. stavka 4. GDPR-a ne može biti osnova

za obradu u druge svrhe (npr. aktivnosti izravnog marketinga). Prava i slobode tih ispitanika koji su tihe strane neće se poštovati ako novi voditelj obrade podataka upotrebljava osobne podatke u druge svrhe, uzimajući u obzir kontekst u kojem su osobni podaci prikupljeni, a posebno nepostojanje bilo kakve veze s ispitanicima koji su tihe strane[29]; nepostojanje bilo kakve veze između bilo koje druge svrhe i svrhe u koju su osobni podaci prvotno prikupljeni (tj. činjenica da pružatelji platnih usluga trebaju podatke tihe strane samo za izvršenje ugovora s drugom ugovornom strankom); prirodu odnosnih osobnih podataka[30], činjenicu da ispitanici nisu u položaju da razumno očekuju daljnju obradu ili čak da znaju koji voditelj obrade možda obrađuje njihove osobne podatke i s obzirom na pravna ograničenja obrade utvrđena u članku 66. stavku 3. točki (g) i članku 67. stavku 2. točki (f) Druge direktive o platnim uslugama.

[29] U uvodnoj izjavi 87. Druge direktive o platnim uslugama navodi se da se ona odnosi samo na „ugovorne obveze i odgovornosti između korisnika platnih usluga i pružatelja platnih usluga". Podaci tihe strane stoga nisu obuhvaćeni područjem primjene Druge direktive o platnim uslugama.

[30] Poseban oprez potreban je kod obrade osobnih financijskih podataka jer se može smatrati da se obradom povećava mogući rizik za prava i slobode pojedinaca, u skladu sa Smjernicama o procjeni učinka na zaštitu podataka.

5. OBRADA POSEBNIH KATEGORIJA OSOBNIH PODATAKA U SKLADU S DRUGOM DIREKTIVOM O PLATNIM USLUGAMA

5.1. Posebne kategorije osobnih podataka

51. Člankom 9. stavkom 1. GDPR-a zabranjuje se obrada „osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca".

52. Potrebno je naglasiti da su u nekim državama članicama elektronička plaćanja već sveprisutna te da im mnogi ljudi u svojim svakodnevnim transakcijama daju prednost pred gotovinom. Istodobno se financijskim transakcijama mogu otkriti osjetljive informacije o ispitaniku, uključujući one koje se odnose na posebne kategorije osobnih podataka. Na primjer, ovisno o pojedinostima transakcije, politička mišljenja i vjerska uvjerenja mogu se otkriti preko donacija političkim strankama ili organizacijama, crkvama ili župama. Članstvo u sindikatu može se otkriti naplatom godišnje članarine s bankovnog računa osobe. Osobni podaci o zdravlju mogu se prikupiti analizom troškova liječenja koje ispitanik plaća medicinskom stručnjaku (na primjer psihijatru). Naposljetku, informacijama o određenim kupovinama mogu se otkriti informacije o seksualnom životu ili spolnoj orijentaciji osobe. Kao što ovi primjeri pokazuju, čak i pojedinačne transakcije mogu sadržavati posebne kategorije osobnih podataka. Osim toga, usluge pružanja informacija o računu mogle bi se oslanjati na izradu profila kako je definirano člankom 4. stavkom 4. GDPR-a. Kako je prethodno navedeno u Smjernicama Radne skupine iz članka 29. o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, kako ih je potvrdio EDPB, „izradom profila mogu se izraditi podaci iz posebne kategorije izvođenjem zaključaka iz podataka koji sami po sebi nisu podaci iz posebne kategorije, no to postaju kad ih se kombinira s drugim podacima."[31] To znači da se pregledom svih financijskih transakcija mogu otkriti različite vrste obrazaca ponašanja, što može uključivati posebne kategorije osobnih podataka. Stoga postoji velika vjerojatnost da pružatelj usluga koji obrađuje informacije o financijskim transakcijama ispitanika obrađuje i posebne kategorije osobnih podataka.

53. U pogledu pojma „osjetljivi podaci o plaćanju" EDPB napominje sljedeće. Definicija osjetljivih podataka o plaćanju u Drugoj direktivi o platnim uslugama znatno se razlikuje od načina na koji se pojam „osjetljivi osobni podaci" obično upotrebljava u kontekstu GDPR-a i (prava) o zaštiti podataka. Ako se u Drugoj direktivi o platnim uslugama „osjetljivi podaci o plaćanju" definiraju kao „podaci, uključujući personalizirane sigurnosne podatke, koji se mogu koristiti za izvršenje prijevare", GDPR-om se naglašava potreba za specifičnom zaštitom posebnih kategorija osobnih podataka koje su prema članku 9. GDPR-a po svojoj prirodi osobito osjetljive u pogledu temeljnih prava i sloboda, kao što su posebne kategorije osobnih podataka[32]. U tom se pogledu preporučuje barem mapiranje i precizno kategoriziranje vrsta osobnih podataka koji će se obrađivati. Najvjerojatnije će biti potrebna procjena učinka na zaštitu podataka u skladu s člankom 35. GDPR-a, što će pomoći u mapiranju. Više uputa o procjeni učinka na zaštitu podataka može se pronaći u Smjernicama Radne Skupine iz članka 29. o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679, kako ih je

[31] Radna skupina iz članka 29., Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, WP251 rev.01, str. 15.

[32] Na primjer, u uvodnoj izjavi 10. GDPR-a posebne kategorije osobnih podataka nazivaju se „osjetljivi podaci".

potvrdio EDPB.

5.2. Moguća odstupanja

54. Zabrana iz članka 9. GDPR-a nije apsolutna. Konkretno, budući da odstupanja iz članka 9. stavka 2. točaka od (b) do (f) i od (h) do (j) GDPR-a očito nisu primjenjiva na obradu osobnih podataka u kontekstu Druge direktive o platnim uslugama, mogla bi se razmotriti sljedeća dva odstupanja iz članka 9. stavka 2. GDPR-a:

a) Zabrana se ne primjenjuje ako je ispitanik dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha (članak 9. stavak 2. točka (a) GDPR-a).

b) Zabrana se ne primjenjuje ako je obrada nužna za potrebe značajnoga javnog interesa na temelju prava Unije ili prava države članice koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika (članak 9. stavak 2. točka (g) GDPR-a).

55. Treba istaknuti da je popis odstupanja iz članka 9. stavka 2. GDPR-a iscrpan. Pružatelj usluga mora priznati mogućnost uključivanja posebnih kategorija osobnih podataka u osobne podatke koji se obrađuju radi pružanja bilo koje usluge obuhvaćene Drugom direktivom o platnim uslugama. Budući da se zabrana iz članka 9. stavka 1. GDPR-a primjenjuje na te pružatelje usluga, oni moraju osigurati da se na njih primjenjuje jedna od iznimaka iz članka 9. stavka 2. GDPR-a. Treba naglasiti da se zabrana iz članka 9. stavka 1. primjenjuje ako pružatelj usluga ne može dokazati da je ispunjeno jedno od odstupanja.

5.3. Značajan javni interes

56. Platnim uslugama mogu se obrađivati posebne kategorije osobnih podataka zbog značajnoga javnog interesa, ali samo ako su ispunjeni svi uvjeti iz članka 9. stavka 2. točke (g) GDPR-a. To znači da se obrada posebnih kategorija osobnih podataka mora rješavati posebnim odstupanjem od članka 9. stavka 1. GDPR-a u pravu Unije ili pravu države članice. Ta odredba morat će se baviti proporcionalnošću u odnosu na željeni cilj obrade te sadržavati odgovarajuće i posebne mjere za zaštitu temeljnih prava i interesa ispitanika. Nadalje, tom odredbom iz prava Unije ili prava države članice morat će se poštovati bit prava na zaštitu podataka. Naposljetku, mora se dokazati da je obrada posebnih kategorija podataka nužna i zbog značajnog javnog interesa, uključujući interese od sistemske važnosti. To se odstupanje može primijeniti na određene vrste platnih usluga samo ako su svi ti uvjeti u potpunosti ispunjeni.

5.4. Izričita privola

57. U slučajevima kada se ne primjenjuje odstupanje iz članka 9. stavka 2. točke (g) GDPR-a, čini se da je dobivanje izričite privole u skladu s uvjetima za valjanu privolu iz GDPR-a jedino moguće zakonito odstupanje na temelju kojeg treće strane koje su pružatelji usluga mogu obrađivati posebne kategorije osobnih podataka. U Smjernicama EDPB-a 5/2020 o privoli na temelju Uredbe 2016/679 navodi se[33] sljedeće: „U članku 9. stavku 2., kao iznimka od opće zabrane obrade posebnih kategorija podataka ne navodi se tekst ‚nužna za izvršenje ugovora'. Stoga bi voditelji obrade i države članice u tom slučaju trebali istražiti posebne iznimke navedene u članku 9. stavku 2. točkama od (b) do (j)." Ako se pružatelji usluga oslanjaju na članak 9. stavak 2. točku (a) GDPR-a, prije nego što započnu s obradom moraju biti sigurni da su dobili izričitu privolu. Izričita privola iz članka 9. stavka 2. točke (a) GDPR-a mora zadovoljavati sve zahtjeve iz GDPR-a.

[33] Smjernice 5/2020 o privoli na temelju Uredbe 2016/679, EDPB, točka 99.

5.5. Nema odgovarajućeg odstupanja

58. Kako je prethodno navedeno, ako pružatelj usluga ne može dokazati da je ispunjeno jedno od odstupanja, primjenjuje se zabrana iz članka 9. stavka 1. U tom bi se slučaju mogle uvesti tehničke mjere za sprječavanje obrade posebnih kategorija osobnih podataka, primjerice sprječavanjem obrade određenih točaka podataka. U tom pogledu pružatelji platnih usluga mogu istražiti tehničke mogućnosti isključivanja posebnih kategorija osobnih podataka i omogućiti odabrani pristup kojim bi se trećim stranama koje su pružatelji usluga onemogućila obrada posebnih kategorija osobnih podataka povezanih s tihim stranama.

6. SMANJENJE KOLIČINE PODATAKA, SIGURNOST, TRANSPARENTNOST, ODGOVORNOST I IZRADA PROFILA

6.1. Smanjenje količine podataka i tehnička i integrirana zaštita podataka

59. Načelo smanjenja količine podataka sadržano je u članku 5. stavku 1. točki (c) GDPR-a: „Osobni podaci moraju biti [...] primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju". U osnovi, u skladu s načelom smanjenja količine podataka, voditelji obrade ne bi smjeli obrađivati više osobnih podataka nego što je potrebno za ostvarivanje konkretne svrhe o kojoj je riječ. Kako je istaknuto u poglavlju 2., iznos i vrsta osobnih podataka potrebnih za pružanje platne usluge određeni su objektivnom ugovornom svrhom o kojoj postoji obostrano razumijevanje[34]. Smanjenje količine podataka primjenjivo je na svaku obradu (npr. svako prikupljanje osobnih podataka ili pristup njima te zahtjev za osobne podatke). U Smjernicama EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka na temelju članka 25. navodi se da su „izvršitelji obrade i pružatelji tehnoloških usluga prepoznati i kao ključni pokretači tehničke i integrirane zaštite podataka te bi trebali biti svjesni i da voditelji obrade moraju obrađivati osobne podatke samo sa sustavima i tehnologijama koji imaju ugrađenu zaštitu podataka"[35].

60. Članak 25. GDPR-a sadržava obveze primjene tehničke i integrirane zaštite podataka. Te su obveze od posebne važnosti za načelo smanjenja količine podataka. Tim se člankom utvrđuje da voditelji obrade u trenutku određivanja sredstava obrade i u trenutku same obrade provode odgovarajuće tehničke i organizacijske mjere osmišljene za učinkovitu provedbu načela zaštite podataka i integraciju potrebnih zaštitnih mjera u obradu kako bi se ispunili zahtjevi GDPR-a i zaštitila prava ispitanika. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da se integriranim načinom obrađuju samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Te mjere mogu uključivati enkripciju, pseudonimizaciju i druge tehničke mjere.

61. Pri primjeni obveze iz članka 25. GDPR-a elementi koje je potrebno uzeti u obzir odnose se na najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade. Dodatna pojašnjenja te obveze navedena su u prethodno navedenim Smjernicama EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka na temelju članka 25.

6.2. Mjere za smanjenje količine podataka

62. Treća strana koja je pružatelj usluga, a koja pristupa podacima o računima za plaćanje radi pružanja traženih usluga, mora uzeti u obzir i načelo smanjenja količine podataka i prikupljati samo one osobne podatke koji su potrebni za pružanje određenih platnih usluga koje je zatražio korisnik platnih usluga. U načelu bi pristup osobnim podacima trebao biti ograničen na ono što je nužno za pružanje platnih usluga. Kao što je prikazano u poglavlju 2., Drugom direktivom o platnim uslugama od ASPSP-a se zahtijeva da na zahtjev korisnika platnih usluga dijele informacije o korisniku platnih usluga kada korisnik platnih usluga želi koristiti uslugu iniciranja plaćanja ili uslugu pružanja informacija o računu.

[34] Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) GDPR-a u kontekstu pružanja internetskih usluga ispitanicima, točka 32.
[35] Smjernice 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., str. 29.

63. Ako za pružanje ugovora nisu potrebni svi podaci o računu za plaćanje, AISP bi prije prikupljanja podataka trebao odabrati relevantne kategorije podataka. Primjerice, kategorije podataka koje možda nisu potrebne mogu obuhvaćati identitet tihe strane i obilježja transakcije. Osim toga, ako to ne zahtijeva pravo države članice ili EU-a, možda neće biti potrebno prikazivati IBAN bankovnog računa tihe strane.

64. U tom bi se pogledu, u skladu s člankom 24. stavkom 2. GDPR-a, mogla razmotriti moguća primjena tehničkih mjera kojima se trećim stranama koje su pružatelji usluga omogućuje ispunjavanje obveze pristupa i preuzimanja samo osobnih podataka potrebnih za pružanje njihovih usluga ili im se u tome pruža podrška, kao dio provedbe odgovarajućih politika zaštite podataka. U tom pogledu EDPB preporučuje upotrebu digitalnih alata kako bi se AISP-ima pružila podrška u ispunjavanju obveze da prikupljaju samo osobne podatke koji su nužni za svrhe u koje se obrađuju. Na primjer, ako pružatelju usluga za pružanje usluge nisu potrebne značajke transakcije (u polju za opis evidencije o transakcijama), alat za digitalni odabir mogao bi trećim stranama koje su pružatelji usluga služiti kao sredstvo za isključivanje tog polja iz ukupnih postupaka obrade koje provodi ta treća strana.

Primjer 2.:

HappyPayments, naš pružatelj usluga pružanja informacija o računu iz primjera 1., želi osigurati da obrađuje samo osobne podatke o računu za plaćanje za koje su njegovi korisnici zainteresirani. Traženje pristupa većem broju podataka o računima za plaćanje ne bi bilo potrebno za pružanje usluge. Stoga omogućuje korisnicima da odaberu posebne vrste informacija za koje su zainteresirani.

Korisnik A želi pregled svoje potrošnje za posljednja dva mjeseca. Stoga za svoja dva bankovna računa koja vode dva različita ASPSP-a traži informacije o svim transakcijama u posljednja dva mjeseca, iznos transakcije, datum izvršenja i ime primatelja te označuje odgovarajuća polja na korisničkom sučelju aplikacije HappyPayments.

HappyPayments zatim počinje od dotičnih ASPSP-a tražiti samo informacije koje odgovaraju poljima koja je odredio korisnik A i samo za razdoblje od posljednja dva mjeseca. Informacije kao što su „priopćavanje" prijenosa, pa čak ni IBAN, nisu zatražene jer ih korisnik A nije tražio.

Kako bi se društvu HappyPayments omogućilo da ispuni svoje obveze smanjenja količine podataka, ASPSP-i omogućuju mu da za niz datuma zatraži posebna polja.

65. U tom pogledu treba napomenuti i da je u skladu s Drugom direktivom o platnim uslugama ASPSP-ima dopušteno samo omogućiti pristup informacijama o računu za plaćanje. U Drugoj direktivi o platnim uslugama ne postoji pravna osnova za omogućivanje pristupa osobnim podacima koje sadržavaju drugi računi, kao što su štedni računi, hipoteke ili investicijski računi. U skladu s time, na temelju Druge direktive o platnim uslugama moraju se provesti tehničke mjere kako bi se osiguralo da pristup bude ograničen na potrebne informacije o računu za plaćanje.

66. Osim prikupljanja što je moguće manje podataka, pružatelj usluga mora primjenjivati i ograničenje razdoblja zadržavanja. Pružatelj usluga ne bi trebao pohranjivati osobne podatke dulje nego što je to potrebno s obzirom na svrhe u koje je korisnik platnih usluga to zatražio.

67. Ako ugovor između ispitanika i AISP-a zahtijeva prijenos osobnih podataka trećim stranama, tada se mogu prenijeti samo oni osobni podaci koji su potrebni za izvršenje ugovora. Ispitanike bi trebalo i posebno obavijestiti o prijenosu i osobnim podacima koji će se prenijeti toj trećoj strani.

6.3. Sigurnost

68. EDPB je već naglasio da povreda osobnih financijskih podataka „očito podrazumijeva ozbiljne učinke na svakodnevni život ispitanika" i kao primjer navodi rizik od prijevare u platnom prometu[36].

69. Ako se povreda podataka odnosi na financijske podatke, ispitanik može biti izložen znatnim rizicima. Ovisno o informacijama koje procure u javnost, ispitanici mogu biti izloženi riziku od krađe identiteta, sredstava na svojim računima i druge imovine. Nadalje, postoji mogućnost da je izloženost podataka o transakcijama povezana sa znatnim rizicima za privatnost jer podaci o transakcijama mogu sadržavati upućivanja na sve aspekte privatnog života ispitanika. Istodobno, financijski podaci očito su vrijedni kriminalcima, stoga su i atraktivna meta.

70. Kao voditelji obrade pružatelji platnih usluga obvezni su poduzeti odgovarajuće mjere za zaštitu osobnih podataka ispitanika (članak 24. stavak 1. GDPR-a). Što su veći rizici povezani s aktivnošću obrade koju provodi voditelj obrade, to su viši sigurnosni standardi koje je potrebno primijeniti. Budući da je obrada financijskih podataka povezana s nizom ozbiljnih rizika, sigurnosne mjere trebale bi biti odgovarajuće visoke.

71. Pružatelji usluga trebali bi ispunjavati visoke standarde, uključujući pouzdane mehanizme autentifikacije klijenta i visoke sigurnosne standarde za tehničku opremu[37]. Važni su i drugi postupci, kao što je provjera sigurnosnih standarda izvršitelja obrade i provedba postupaka protiv neovlaštenog pristupa.

6.4. Transparentnost i odgovornost

72. Transparentnost i odgovornost dva su temeljna načela GDPR-a.

73. Kad je riječ o transparentnosti (članak 5. stavak 1. točka (a) GDPR-a), u članku 12. GDPR-a navodi se da voditelji obrade poduzimaju odgovarajuće mjere za pružanje svih informacija iz članaka 13. i 14. GDPR-a. Nadalje, njime se zahtijeva da informacije ili komunikacije o obradi osobnih podataka budu sažete, transparentne, razumljive i lako dostupne. Informacije moraju biti na jasnom i jednostavnom jeziku te u pisanom obliku „ili drugim sredstvima, među ostalim, ako je prikladno, elektroničkim putem". Smjernicama Radne skupine iz članka 29. o transparentnosti na temelju Uredbe 2016/679, kako ih je odobrio EDPB, daju se posebne upute za usklađenost s načelom transparentnosti u digitalnim okruženjima.

74. U skladu s prethodno navedenim Smjernicama o transparentnosti na temelju Uredbe 2016/679, članak 11. GDPR-a trebalo bi tumačiti kao način provedbe istinskog smanjenja količine podataka bez ometanja ostvarivanja prava ispitanika te bi ostvarivanje prava ispitanika trebalo omogućiti uz pomoć dodatnih informacija koje pruža ispitanik. Mogu nastati situacije u kojima voditelj obrade podataka obrađuje osobne podatke za koje nije potrebna identifikacija ispitanika (na primjer sa pseudonimiziranim podacima). U takvim bi slučajevima mogao biti relevantan i članak 11. stavak 1. jer se u njemu navodi da voditelj obrade nije obvezan zadržavati, stjecati ili obrađivati dodatne informacije radi identificiranja ispitanika samo u svrhu poštovanja GDPR-a.

75. Na usluge iz Druge direktive o platnim uslugama primjenjuje se članak 13. GDPR-a za osobne podatke prikupljene od ispitanika, a članak 14. primjenjuje se ako osobni podaci nisu dobiveni od ispitanika.

76. Konkretno, ispitanika se mora obavijestiti o razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, o kriterijima korištenima za određivanje tog razdoblja te, ako je primjenjivo, o

[36] Smjernice Radne skupine iz članka 29. o procjeni učinka na zaštitu podataka i utvrđivanju vjerojatnosti da će obrada „prouzročiti visok rizik" u smislu Uredbe 2016/679, WP248 rev.01 – odobrio EDPB.
[37] Vidjeti Delegiranu uredbu Komisije (EU) 2018/389.

legitimnim interesima voditelja obrade ili moguće treće strane. Ako se obrada temelji na privoli iz članka 6. stavka 1. točke (a) GDPR-a ili izričitoj privoli iz članka 9. stavka 2. točke (a) GDPR-a, ispitanika se mora obavijestiti o tome da ima pravo na povlačenje privole u bilo koje vrijeme.

77. Voditelj obrade pruža informacije ispitaniku, uzimajući u obzir posebne okolnosti u kojima se osobni podaci obrađuju. Ako će se osobni podaci upotrebljavati za komunikaciju s ispitanikom[38], što će vjerojatno biti slučaj kod AISP-a, informacije se moraju pružiti najkasnije u trenutku prvog priopćavanja tom ispitaniku. Ako se osobni podaci otkrivaju drugom primatelju, informacije se moraju dostaviti najkasnije prilikom prvog otkrivanja osobnih podataka.

78. Kad je riječ o uslugama plaćanja na internetu, u prethodno navedenim smjernicama pojašnjava se da voditelji obrade podataka mogu slijediti slojeviti pristup ako odluče upotrebljavati kombinaciju metoda za osiguravanje transparentnosti. Posebno se preporučuje da se slojevite izjave/obavijesti o privatnosti upotrebljavaju za pružanje poveznica na razne kategorije informacija koje se moraju pružati ispitaniku, umjesto da se sve te informacije prikazuju u jednoj obavijesti na ekranu, kako bi se izbjeglo umaranje zbog prekomjernih informacija i istodobno osigurala učinkovitost informacija.

79. U prethodno navedenim smjernicama pojašnjava se i da voditelji obrade mogu odabrati i primjenu dodatnih alata za transparentnost kojima se pojedinačnom ispitaniku pružaju informacije, poput nadzornih ploča za privatnost. Nadzorna ploča za privatnost jedinstvena je točka na kojoj ispitanici mogu pregledavati „informacije o privatnosti" i upravljati svojim postavkama privatnosti tako da dopuštaju ili sprječavaju određeni način upotrebljavanja svojih podataka u okviru predmetne usluge[39]. Nadzornom pločom za privatnost mogao bi se ponuditi pregled trećih stana koje su pružatelji usluga, a koje su dobile izričitu suglasnost ispitanika. Mogle bi se ponuditi i relevantne informacije o prirodi i količini osobnih podataka kojima su pristupili ti pružatelji usluga. U načelu, ASPSP može korisniku ponuditi mogućnost povlačenja izričite suglasnosti[40] na temelju Druge direktive o platnim uslugama putem pregleda, što bi dovelo do uskraćivanja pristupa jedne ili više trećih strana koje su pružatelji usluga njihovim računima za plaćanja. Korisnik može zatražiti i od ASPSP-a da jednoj ili više određenih trećih strana koje su pružatelji usluga[41] uskrati pristup njegovim računima za plaćanje jer korisnik ima pravo (ne) koristiti uslugu pružanja informacija o računu. Ako se za davanje ili povlačenje izričite suglasnosti upotrebljavaju nadzorne ploče za privatnost, one bi trebale biti osmišljene i primijenjene u skladu sa zakonom, a posebno bi trebale sprječavati nastanak prepreka za treće strane koje su pružatelji usluga u pogledu njihova prava na pružanje usluga u skladu s Drugom direktivom o platnim uslugama. U tom pogledu i u skladu s primjenjivim odredbama Druge direktive o platnim uslugama, treća strana koja je pružatelj usluga ima mogućnost od korisnika ponovno dobiti izričitu suglasnost nakon što je ta suglasnost povučena.

80. U skladu s načelima odgovornosti voditelj obrade mora utvrditi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s GDPR-om,

[38] Članak 14. stavak 3. točka (b) GDPR-a.

[39] U skladu sa Smjernicama Radne skupine iz članka 29. o transparentnosti na temelju Uredbe 2016/679, koje je odobrio EDPB, nadzorne ploče za zaštitu privatnosti osobito su korisne ako ispitanici koriste istu uslugu na nizu različitih uređaja jer im je time omogućen pristup njihovim osobnim podacima i nadzor nad njima neovisno o načinu korištenja usluge. Ako se ispitanicima omogući da ručno prilagođavaju svoje postavke privatnosti preko nadzorne ploče za privatnost, može se olakšati i personalizacija izjave/obavijesti o privatnosti tako da ona odražava samo one vrste obrade koje se provode za tog konkretnog ispitanika.

[40] Vidjeti, na primjer, „izričitu suglasnost" iz članka 67. stavka 2. točke (a) Druge direktive o platnim uslugama.

[41] Vidjeti i EBA/OP/2020/10, točka 45.

posebno s glavnim načelima zaštite podataka iz članka 5. stavka 1. Kod tih bi se mjera trebali uzeti u obzir priroda, opseg, kontekst i svrhe obrade te rizik za prava i slobode pojedinaca te ih prema potrebi treba preispitati i ažurirati[42].

6.5. Izrada profila

81. Obrada osobnih podataka koju provode pružatelji platnih usluga može podrazumijevati „izradu profila" kako je navedeno u članku 4. stavku 4. GDPR-a. Na primjer, AISP-i bi se mogli oslanjati na automatiziranu obradu osobnih podataka kako bi ocijenili određene osobne aspekte povezane s fizičkom osobom. Mogla bi se ocjenjivati osobna financijska situacija ispitanika, ovisno o specifičnostima usluge. Usluge pružanja informacija o računu koje se pružaju na zahtjev korisnika mogu obuhvaćati opsežnu procjenu osobnih podataka o računu za plaćanja.

82. Voditelj obrade mora biti transparentan prema ispitaniku i u pogledu postojanja automatiziranog donošenja odluka, uključujući izradu profila. U tim slučajevima voditelj obrade mora pružiti smislene informacije i o tome o kojoj je logici riječ, kao i važnost te predviđene posljedice takve obrade za ispitanika (članak 13. stavak 2. točka (f), članak 14. stavak 2. točka (g) i uvodna izjava 60.)[43]. Isto tako, na temelju članka 15. GDPR-a ispitanik ima pravo od voditelja obrade zatražiti i dobiti informacije o postojanju automatiziranog donošenja odluka, što uključuje izradu profila, o tome o kojoj je logici riječ i posljedicama za ispitanika te, u određenim okolnostima, o pravu na prigovor na izradu profila, neovisno o tome provodi li se automatizirano pojedinačno donošenje odluka isključivo na temelju izrade profila[44].

83. Nadalje, u tom je kontekstu relevantno i pravo ispitanika da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, kako je predviđeno člankom 22. GDPR-a. Ta norma uključuje, u određenim okolnostima, i potrebu da voditelji obrade podataka provedu odgovarajuće mjere za zaštitu prava ispitanika, kao što su davanje određenih informacija ispitaniku te pravo na ljudsku intervenciju u donošenju odluka, izražavanje vlastitog stajališta i osporavanje odluke. Kako je navedeno i u uvodnoj izjavi 71. GDPR-a, to znači, među ostalim, da ispitanici imaju pravo na to da se na njih ne odnosi odluka, poput automatskog odbijanja zahtjeva za kredit putem interneta bez ikakve ljudske intervencije[45].

84. Automatizirano donošenje odluka, uključujući izradu profila, koje uključuje posebne kategorije osobnih podataka, dopušta se samo pod kumulativnim uvjetima iz članka 22. stavka 4. GDPR-a:

- postoji primjenjiva iznimka iz članka 22. stavka 2.
- i primjenjuje se članak 9. stavak 2. točka (a) ili (g) GDPR-a. U oba slučaja voditelj obrade uspostavlja odgovarajuće mjere za zaštitu prava i sloboda te legitimnih interesa ispitanika[46].

85. Trebalo bi poštovati i zahtjeve za daljnju obradu, kako je navedeno u ovim Smjernicama. Pojašnjenja i upute o automatiziranom pojedinačnom donošenju odluka i izradi profila navedeni u Smjernicama Radne skupine iz članka 29. o automatiziranom pojedinačnom donošenju odluka i

[42] Članak 5. stavak 2. i članak 24. GDPR-a.
[43] Smjernice o transparentnosti na temelju Uredbe 2016/679, WP260 rev.01 – odobrio EDPB.
[44] Smjernice Radne skupine iz članka 29. o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, WP251 rev.01.
[45] Uvodna izjava 71. GDPR-a.
[46] Smjernice Radne skupine iz članka 29. o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, WP251 rev.01, stranica 24.

izradi profila za potrebe Uredbe 2016/679, kako ih je odobrio EDPB, u potpunosti su relevantni u kontekstu platnih usluga te bi ih stoga trebalo propisno razmotriti.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)