Smernice št. 6/2020 o medsebojnem vplivu druge direktive o plačilnih storitvah in Splošne uredbe o varstvu podatkov

Različica 2.0

Sprejete 15. decembra 2020

Zgodovina različic

Različica 2.0	15. december 2020	Sprejetje smernic po javnem posvetovanju
Različica 1.0	17. julij 2020	Sprejetje smernic za javno posvetovanje

Kazalo

1 Uvod 5

1.1 Opredelitev pojmov 6

1.2 Storitve v okviru direktive PSD2 7

2 Zakoniti razlogi in nadaljnja obdelava v skladu z direktivo PSD2 10

2.1 Zakoniti razlogi za obdelavo 10

2.2 Člen 6(1)(b) Splošne uredbe o varstvu podatkov (obdelava je potrebna za izvajanje pogodbe) 10

2.3 Preprečevanje goljufij 12

2.4 Nadaljnja obdelava (ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil) 12

2.5 Zakonit razlog za omogočanje dostopa do računa (ponudniki plačilnih storitev, ki vodijo račune) 13

3 Izrecna privolitev OZIROMA soglasje 14

3.1 Privolitev v skladu s Splošno uredbo o varstvu podatkov 14

3.2 Soglasje v skladu z direktivo PSD2 14

3.2.1 Izrecno soglasje iz člena 94(2) direktive PSD2 15

3.3 Sklep 16

4 Obdelava podatkov tihe stranke 18

4.1 Podatki tihe stranke 18

4.2 Zakoniti interes upravljavca 18

4.3 Nadaljnja obdelava osebnih podatkov tihe stranke 18

5 Obdelava posebnih vrst osebnih podatkov v skladu z direktivo PSD2 20

5.1 Posebne vrste osebnih podatkov 20

5.2 Možna odstopanja 21

5.3 Bistven javni interes 21

5.4 Izrecna privolitev 21

5.5 Ni ustreznega odstopanja 22

6 Najmanjši obseg podatkov, varnost, preglednost, odgovornost in oblikovanje profilov 23

6.1 Najmanjši obseg podatkov ter vgrajeno in privzeto varstvo podatkov 23

6.2 Ukrepi za najmanjši obseg podatkov 23

6.3 Varnost 25

6.4 Preglednost in odgovornost 25

6.5 Oblikovanje profilov 27

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika,

ob upoštevanju naslednjega:

(1) Splošna uredba o varstvu podatkov zagotavlja usklajen sklop pravil za obdelavo osebnih podatkov v EU.

(2) Druga direktiva o plačilnih storitvah (Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 23. decembra 2015, v nadaljevanju: direktiva PSD2) razveljavlja Direktivo 2007/64/ES ter določa nova pravila, ki potrošnikom, trgovcem in podjetjem zagotavljajo pravno varnost v plačilni verigi in posodabljajo pravni okvir za trg plačilnih storitev[2]. Države članice so morale direktivo PSD2 v nacionalno pravo prenesti do 13. januarja 2018.

(3) Pomembna značilnost direktive PSD2 je uvedba pravnega okvira za nove storitve odreditve plačil in storitve zagotavljanja informacij o računih. Direktiva PSD2 ponudnikom teh novih plačilnih storitev omogoča pridobivanje dostopa do plačilnih računov posameznikov, na katere se nanašajo osebni podatki, za zagotavljanje navedenih storitev.

(4) Glede varstva podatkov se v skladu s členom 94(1) direktive PSD2 kakršna koli obdelava osebnih podatkov, vključno z obveščanjem o obdelavi, za namene direktive PSD2 izvaja v skladu s Splošno uredbo o varstvu podatkov[3] in Uredbo (EU) 2018/1725.

(5) V uvodni izjavi 89 direktive PSD2 je navedeno, da bi bilo treba v primeru obdelave osebnih podatkov za namene direktive PSD2 določiti natančen namen obdelave, navesti zadevno pravno podlago, upoštevati ustrezne varnostne zahteve iz Splošne uredbe o varstvu podatkov ter spoštovati načela nujnosti, sorazmernosti, omejitve namena in sorazmernega obdobja hrambe podatkov. Poleg tega bi morali imeti vsi sistemi za obdelavo podatkov, ki se razvijejo in uporabljajo v okviru direktive PSD2, vgrajene funkcije za varstvo podatkov in slednje zagotavljati privzeto[4].

(6) V uvodni izjavi 93 direktive PSD2 je navedeno, da bi morali ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih na eni strani ter ponudnik plačilnih storitev, ki vodi račun, na drugi strani izpolnjevati ustrezne zahteve glede varstva podatkov in varnosti, določene ali omenjene v direktivi PSD2 ali vključene v regulativne tehnične standarde –

[1] Sklicevanja na „države članice“ v tem dokumentu je treba razumeti kot sklicevanja na „države članice EGP“.
[2] Uvodna izjava 6 direktive PSD2.
[3] Ker je bila direktiva PSD2 sprejeta prej kot Splošna uredba o varstvu podatkov, se še vedno sklicuje na Direktivo 95/46/ES. Člen 94 Splošne uredbe o varstvu podatkov določa, da se sklicevanja na razveljavljeno Direktivo 95/46/ES štejejo kot sklicevanja na Splošno uredbo o varstvu podatkov.
[4] Uvodna izjava 89 direktive PSD2.

SPREJEL NASLEDNJE SMERNICE:

1 UVOD

1. Druga direktiva o plačilnih storitvah (v nadaljevanju: direktiva PSD2) je prinesla več novosti na področju plačilnih storitev. Direktiva PSD2 za potrošnike ustvarja nove priložnosti in izboljšuje preglednost na tem področju, hkrati pa njena uporaba poraja nekatera vprašanja in vzbuja pomisleke glede potrebe, da posamezniki, na katere se nanašajo osebni podatki, ohranijo popoln nadzor nad svojimi osebnimi podatki. Splošna uredba o varstvu podatkov se uporablja za obdelavo osebnih podatkov, vključno z dejavnostmi obdelave, izvedenimi v okviru plačilnih storitev, kot jih opredeljuje direktiva PSD2[5]. Zato morajo upravljavci, dejavni na področju, ki ga zajema direktiva PSD2, vedno zagotoviti skladnost z zahtevami Splošne uredbe o varstvu podatkov, vključno z načeli varstva podatkov iz člena 5 Splošne uredbe o varstvu podatkov, ter ustreznimi določbami direktive o e-zasebnosti[6]. Direktiva PSD2[7] ter regulativni tehnični standardi za močno avtentikacijo strank ter skupne in varne odprte standarde komunikacije (v nadaljevanju: RTS[8]) vsebujejo nekatere določbe v zvezi z varstvom in varnostjo podatkov, vendar pa se je pojavila negotovost glede razlage teh določb in tudi glede medsebojnega vpliva splošnega okvira za varstvo podatkov in direktive PSD2.

2. Evropski odbor za varstvo podatkov je 5. julija 2018 sprejel dopis v zvezi z direktivo PSD2, v katerem je podal pojasnila glede vprašanj o varstvu osebnih podatkov v povezavi z direktivo PSD2, zlasti glede obdelave osebnih podatkov nepogodbenic (tako imenovanih podatkov tihe stranke), ki jo izvajajo ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil, postopkov v zvezi z dajanjem in umikom soglasja, RTS in sodelovanjem med ponudniki plačilnih storitev, ki vodijo račune, glede varnostnih ukrepov. Priprava za te smernice je vključevala zbiranje mnenj deležnikov v pisni obliki ter na srečanju deležnikov, da bi se opredelili najbolj pereči izzivi.

3. Namen teh smernic je zagotoviti nadaljnje usmeritve o vidikih varstva podatkov v okviru direktive PSD2, zlasti o razmerju med zadevnimi določbami Splošne uredbe o varstvu podatkov in direktive PSD2. Te smernice se nanašajo zlasti na obdelavo osebnih podatkov, ki jo izvajajo ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil. Zato ta dokument obravnava pogoje za omogočanje dostopa do informacij o plačilnih računih ponudnikom plačilnih storitev, ki vodijo račune, ter za obdelavo osebnih podatkov, ki jo izvajajo ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih, vključno z zahtevami in zaščitnimi ukrepi glede obdelave osebnih podatkov, ki jo izvajajo ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih za namene, ki niso prvotni nameni,

[5] Člen 1(1) Splošne uredbe o varstvu podatkov.
[6] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31. 7. 2002, stran 37).
[7] Člen 94 direktive PSD itd.
[8] Delegirana uredba Komisije (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije (Besedilo velja za EGP) (C(2017) 7782; UL L 69, 13. 3. 2018, stran 23), na voljo na povezavi https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32018R0389&from=EN.

za katere so se podatki zbirali, zlasti če so bili zbrani v okviru zagotavljanja informacij o računih[9]. Ta dokument obravnava tudi različna pojma „izrecno soglasje“ iz direktive PSD2 in „izrecna privolitev“ iz Splošne uredbe o varstvu podatkov, obdelavo „podatkov tihe stranke“, obdelavo posebnih vrst osebnih podatkov, ki jo izvajajo ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih, ter uporabo glavnih načel varstva podatkov iz Splošne uredbe o varstvu podatkov, vključno z najmanjšim obsegom podatkov, preglednostjo, odgovornostjo in varnostnimi ukrepi. Direktiva PSD2 vključuje večfunkcijske odgovornosti med drugim na področjih varstva potrošnikov in konkurenčnega prava. Premisleki glede teh področij prava presegajo področje uporabe teh smernic.

4. Za lažje branje teh smernic so v nadaljevanju navedene glavne opredelitve pojmov, ki se uporabljajo v tem dokumentu.

1.1 Opredelitev pojmov

„Ponudnik storitev zagotavljanja informacij o računih“ pomeni ponudnika spletne storitve zagotavljanja konsolidiranih informacij o enem ali več plačilnih računih, ki jih ima uporabnik plačilnih storitev pri drugem ponudniku plačilnih storitev ali več kot enem ponudniku plačilnih storitev.

„Ponudnik plačilnih storitev, ki vodi račun“ pomeni ponudnika plačilnih storitev, ki plačniku zagotavlja plačilni račun in ga zanj vodi.

„Najmanjši obseg podatkov“ je načelo varstva podatkov, v skladu s katerim so osebni podatki ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo.

„Plačnik“ pomeni fizično ali pravno osebo, ki je imetnik plačilnega računa in odobri plačilni nalog v breme navedenega plačilnega računa, ali, če plačilni račun ne obstaja, fizično ali pravno osebo, ki izda plačilni nalog.

„Prejemnik plačila“ pomeni fizično ali pravno osebo, ki je predvideni prejemnik sredstev, ki so bila predmet plačilne transakcije.

„Plačilni račun“ pomeni račun, voden v imenu enega ali več uporabnikov plačilnih storitev, ki se uporablja za izvrševanje plačilnih transakcij.

„Ponudnik storitev odreditve plačil“ pomeni ponudnika storitve za odreditev plačilnega naloga na zahtevo uporabnika plačilnih storitev v zvezi s plačilnim računom, odprtem pri drugem ponudniku plačilnih storitev.

„Ponudnik plačilnih storitev“ pomeni subjekt iz člena 1(1) direktive PSD2[10] ali fizično ali pravno osebo, ki ji je bila odobrena izjema na podlagi člena 32 ali 33 direktive PSD2.

---

[9] Storitev zagotavljanja informacij o računih je spletna storitev za zagotavljanje konsolidiranih informacij o enem ali več plačilnih računih, ki jih ima uporabnik plačilnih storitev pri drugem ponudniku plačilnih storitev ali pri več kot enem ponudniku plačilnih storitev.

[10] V členu 1(1) direktive PSD2 je navedeno, da direktiva PSD2 določa pravila, v skladu s katerimi države članice razlikujejo naslednje kategorije *ponudnikov plačilnih storitev*:
(a) kreditne institucije, kakor so opredeljene v točki (1) člena 4(1) Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta (1), vključno s podružnicami teh institucij v smislu točke (17) člena 4(1) te uredbe, kadar se take podružnice nahajajo v Uniji, ne glede na to, ali je glavni sedež teh podružnic v Uniji ali pa je v skladu s členom 47 Direktive 2013/36/EU in nacionalnim pravom zunaj Unije;
(b) institucije za izdajo elektronskega denarja v smislu točke (1) člena 2 Direktive 2009/110/ES, vključno s podružnicami teh institucij, v skladu s členom 8 navedene direktive in nacionalnim pravom, kadar se take

„Uporabnik plačilnih storitev“ pomeni fizično ali pravno osebo, ki uporablja plačilne storitve kot plačnik ali prejemnik plačila ali oboje.

„Osebni podatki“ pomenijo katero koli informacijo v zvezi z določeno ali določljivo fizično osebo („posameznik, na katerega se nanašajo osebni podatki“); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot so ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, značilnih za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

„Vgrajeno varstvo podatkov“ pomeni tehnične in organizacijske ukrepe, vgrajene v produkt ali storitev, ki so oblikovani za učinkovito izvajanje načel varstva podatkov ter v obdelavo vključijo potrebne zaščitne ukrepe, da se izpolnijo zahteve Splošne uredbe o varstvu podatkov in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

„Privzeto varstvo podatkov“ pomeni ustrezne tehnične in organizacijske ukrepe, vgrajene v produkt ali storitev, s katerimi se zagotovi, da se privzeto obdelajo samo osebni podatki, potrebni za vsak poseben namen obdelave.

„RTS“ pomeni Delegirano uredbo Komisije (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije.

„Tretji ponudniki storitev“ pomeni tako ponudnike storitev odreditve plačil kot tudi ponudnike storitev zagotavljanja informacij o računih.

1.2 Storitve v okviru direktive PSD2

5. Direktiva PSD2 uvaja dve novi vrsti (ponudnikov) plačilnih storitev: ponudnike storitev odreditve plačil in ponudnike storitev zagotavljanja informacij o računih. Priloga I k direktivi PSD2 vsebuje osem plačilnih storitev, ki jih zajema direktiva PSD2.

6. Ponudniki storitev odreditve plačil opravljajo storitve za odreditev plačilnih nalogov na zahtevo uporabnika plačilnih storitev v zvezi s plačilnim računom uporabnika, odprtem pri drugem ponudniku plačilnih storitev[11]. Ponudnik storitev odreditve plačil lahko od ponudnika plačilnih storitev, ki vodi račun (po navadi je to banka), zahteva odreditev transakcije v imenu uporabnika plačilnih storitev. Uporabnik (plačilnih storitev) je lahko fizična oseba (posameznik, na katerega se nanašajo osebni podatki) ali pravna oseba.

7. Ponudniki storitev zagotavljanja informacij o računih zagotavljajo spletne storitve za konsolidirane informacije o enem ali več plačilnih računih, ki jih ima uporabnik plačilnih storitev pri drugem ponudniku plačilnih storitev ali pri več kot enem ponudniku plačilnih storitev[12]. V skladu z uvodno izjavo 28 direktive PSD2 je uporabniku plačilnih storitev omogočeno, da ima v danem trenutku takoj celovit pregled nad svojim finančnim položajem.

podružnice nahajajo v Uniji, njihov glavni sedež pa je zunaj Unije, v kolikor so plačilne storitve, ki jih opravljajo te podružnice, povezane z izdajo elektronskega denarja;
(c) poštne institucije, ki imajo na podlagi nacionalnega prava pravico opravljati plačilne storitve;
(d) plačilne institucije;
(e) ECB in nacionalne centralne banke, kadar ne delujejo kot monetarni organ ali drugi javni organi;
(f) države članice ali njihovi regionalni ali lokalni organi, kadar ne delujejo kot javni organi.

[11] Člen 4(15) direktive PSD2.

[12] Člen 4(16) direktive PSD2.

8. V zvezi s storitvami zagotavljanja informacij o računih je mogoče ponujati več različnih vrst storitev, s poudarkom na različnih značilnostih in namenih. Nekateri ponudniki lahko na primer uporabnikom ponujajo storitve, kot sta načrtovanje proračuna in spremljanje porabe. Obdelavo osebnih podatkov v okviru takih storitev zajema direktiva PSD2. Storitve, ki vključujejo ocene kreditne sposobnosti uporabnika plačilnih storitev ali storitve revizije, ki se izvedejo na podlagi zbirke informacij s storitvijo zagotavljanja informacij o računih, ne spadajo na področje uporabe direktive PSD2, ampak na področje uporabe Splošne uredbe o varstvu podatkov. Poleg tega direktiva PSD2 ne zajema tudi računov, ki niso plačilni računi (na primer varčevalni in naložbeni računi). V vsakem primeru je Splošna uredba o varstvu podatkov veljavni pravni okvir za obdelavo osebnih podatkov.

Primer 1:
HappyPayments je podjetje, ki ponuja spletno storitev, ki zajema zagotavljanje informacij o enem ali več plačilnih računih prek mobilne aplikacije za zagotavljanje nadzora nad finančnimi sredstvi (storitev zagotavljanja informacij o računih). S to storitvijo lahko uporabnik plačilnih storitev takoj preveri stanje in zadnje transakcije na dveh ali več plačilnih računih, odprtih pri različnih bankah. Če uporabnik plačilnih storitev želi, aplikacija omogoča tudi kategorizacijo porabe in prihodkov glede na različne tipologije (plača, prosti čas, energija, hipoteka itd.), kar uporabniku plačilnih storitev pomaga pri finančnem načrtovanju. V tej aplikaciji podjetje HappyPayments ponuja tudi storitev odreditve plačil neposredno z določenih plačilnih računov uporabnika (storitev odreditve plačil).

9. Za opravljanje takih storitev direktiva PSD2 določa pravne pogoje, pod katerimi lahko ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih za opravljanje storitve za uporabnika plačilnih storitev dostopajo do plačilnih računov.

10. Člena 66(1) in 67(1) direktive PSD2 določata, da sta dostop do plačilnih storitev in storitev zagotavljanja informacij o računih ter njihova uporaba pravici uporabnika plačilnih storitev. To pomeni, da bi moral imeti uporabnik plačilnih storitev pri uveljavljanju take pravice popolno svobodo in ga v to ni mogoče prisiliti.

11. Dostop do plačilnih računov in uporabo informacij o plačilnih računih delno urejata člena 66 in 67 direktive PSD2, ki vsebujeta zaščitne ukrepe za varstvo (osebnih) podatkov. V členu 66(3)(f) direktive PSD2 je določeno, da ponudnik storitev odreditve plačil od uporabnika plačilnih storitev ne zahteva nobenih drugih podatkov razen podatkov, ki so potrebni za opravljanje storitve odreditve plačila, v členu 66(3)(g) direktive PSD2 pa je določeno, da ponudnik storitev odreditve plačil podatkov ne uporablja, ne dostopa do njih in jih ne hrani za druge namene kot za namene opravljanja storitve odreditve plačila, ki jo plačnik izrecno zahteva. Poleg tega člen 67(2)(d) direktive PSD2 za ponudnike storitev zagotavljanja informacij o računih dostop omejuje samo do informacij določenih plačilnih računov in s tem povezanih plačilnih transakcij, v členu 67(2)(f) direktive PSD2 pa je določeno, da ponudniki storitev zagotavljanja informacij o računih podatkov ne uporabljajo, ne dostopajo do njih ali jih ne hranijo za druge namene kot za namene opravljanja storitve zagotavljanja informacij o računih, ki jo uporabnik plačilnih storitev izrecno zahteva v skladu s predpisi o varstvu podatkov. Zadnji stavek poudarja, da je mogoče v okviru storitev zagotavljanja informacij o računih osebne podatke zbirati le za določene, izrecne in zakonite namene. Ponudnik storitev zagotavljanja informacij o računih bi moral torej v pogodbi izrecno navesti, za katere določene namene se bodo osebni podatki iz informacij o računih obdelovali v okviru njegovih storitev zagotavljanja informacij o računih. Pogodba bi morala biti zakonita, poštena in pregledna v skladu s členom 5 Splošne uredbe o varstvu podatkov ter skladna z drugo zakonodajo o varstvu potrošnikov.

12. Ponudniki plačilnih storitev so lahko, odvisno od zadevnih okoliščin, upravljavci ali obdelovalci v skladu s Splošno uredbo o varstvu podatkov. V teh smernicah so „upravljavci“ tisti ponudniki plačilnih storitev, ki sami ali skupaj z drugimi določijo namene in sredstva obdelave osebnih podatkov. Več usmeritev glede tega je na voljo v smernicah Evropskega odbora za varstvo podatkov št. 7/2020 o pojmih upravljavec in obdelovalec v Splošni uredbi o varstvu podatkov.

2 ZAKONITI RAZLOGI IN NADALJNJA OBDELAVA V SKLADU Z DIREKTIVO PSD2

2.1 Zakoniti razlogi za obdelavo

13. V skladu s Splošno uredbo o varstvu podatkov morajo imeti upravljavci pravno podlago za obdelavo osebnih podatkov. Člen 6(1) Splošne uredbe o varstvu podatkov vsebuje izčrpen in omejevalen seznam šestih pravnih podlag za obdelavo osebnih podatkov v skladu s Splošno uredbo o varstvu podatkov[13]. Upravljavec je tisti, ki opredeli ustrezno pravno podlago in zagotovi izpolnjevanje vseh pogojev zanjo. Določitev, katera podlaga je veljavna in najustreznejša v specifični situaciji, je odvisna od okoliščin, v katerih obdelava poteka, vključno z namenom obdelave ter razmerjem med upravljavcem in posameznikom, na katerega se osebni podatki nanašajo.

2.2 Člen 6(1)(b) Splošne uredbe o varstvu podatkov (obdelava je potrebna za izvajanje pogodbe)

14. Plačilne storitve se opravljajo na podlagi pogodbe med uporabnikom plačilnih storitev in ponudnikom plačilnih storitev. V uvodni izjavi 87 direktive PSD2 je navedeno: „[t]a direktiva bi se morala nanašati le na pogodbene obveznosti in odgovornosti med uporabnikom plačilnih storitev in ponudnikom plačilnih storitev.“ Pri Splošni uredbi o varstvu podatkov je glavna pravna podlaga za obdelavo osebnih podatkov za opravljanje plačilnih storitev njen člen 6(1)(b), kar pomeni, da je obdelava potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe.

15. Plačilne storitve iz direktive PSD2 so opredeljene v Prilogi I k direktivi PSD2. Zagotavljanje navedenih storitev, kot so opredeljene v direktivi PSD2, je pogoj za sklenitev pogodbe, po kateri imajo pogodbene stranke dostop do podatkov plačilnega računa uporabnika plačilnih storitev. Taki ponudniki plačilnih storitev morajo imeti tudi ustrezno dovoljenje. Kar zadeva storitve odreditve plačil in storitve zagotavljanja informacij o računih iz direktive PSD2, lahko pogodbe vsebujejo pogoje za dodatne storitve, ki jih direktiva PSD2 ne ureja. *Smernice Evropskega odbora za varstvo podatkov 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu*

[13] V skladu s členom 6 je obdelava zakonita le in kolikor je izpolnjen vsaj eden od naslednjih pogojev:

(a) posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;

(b) obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;

(c) obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;

(d) obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;

(e) obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;

(f) obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, jasno navajajo, da morajo upravljavci oceniti, katera obdelava osebnih podatkov je objektivno potrebna za izvajanje pogodbe. Te smernice poudarjajo, da je utemeljitev potrebnosti odvisna od narave storitve, vzajemnih stališč in pričakovanj pogodbenih strank, utemeljitve pogodbe in bistvenih elementov pogodbe.

16. Smernice Evropskega odbora za varstvo podatkov 2/2019 jasno navajajo tudi, da se z vidika člena 7(4) Splošne uredbe o varstvu podatkov razlikuje med dejavnostmi obdelave, potrebnimi za izvajanje pogodbe, in določili, ki storitev pogojujejo z nekaterimi dejavnostmi obdelave, ki za izvajanje pogodbe dejansko niso potrebne. „Potrebno za izvajanje“ jasno zahteva nekaj več kot le pogodbeni pogoj[14]. Upravljavec bi moral biti zmožen dokazati, da glavnega predmeta konkretne pogodbe s posameznikom, na katerega se nanašajo osebni podatki, dejansko ni mogoče izpolniti brez konkretne obdelave zadevnih osebnih podatkov. Zgolj sklicevanje na obdelavo podatkov ali omemba take obdelave v pogodbi ni dovolj, da bi zadevna obdelava spadala na področje uporabe člena 6(1)(b) Splošne uredbe o varstvu podatkov.

17. Člen 5(1)(b) Splošne uredbe o varstvu podatkov določa načelo omejitve namena, v skladu s katerim se morajo osebni podatki zbirati za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni. Pri oceni, ali je člen 6(1)(b) ustrezna pravna podlaga za spletno (plačilno) storitev, je treba upoštevati zadevni smoter, namen ali cilj storitve[15]. Nameni obdelave morajo biti jasno določeni in sporočeni posamezniku, na katerega se nanašajo osebni podatki, v skladu z obveznostmi upravljavca glede omejitev namena in preglednosti. Ocena, kaj je „potrebno“, zajema kombinirano, na dejstvih utemeljeno oceno obdelave „v zvezi s postavljenim ciljem in ali gre pri tem za manjše poseganje kot pri drugih možnostih za dosego istega cilja“. Člen 6(1)(b) ne zajema obdelave, ki je sicer koristna, vendar objektivno ni potrebna za izvajanje pogodbene storitve ali sprejetje zadevnih predpogodbenih ukrepov na zahtevo posameznika, na katerega se nanašajo osebni podatki, čeprav je potrebna za druge upravljavčeve poslovne namene[16].

18. Smernice Evropskega odbora za varstvo podatkov 2/2019 jasno navajajo, da pogodbe ne morejo umetno razširiti kategorij osebnih podatkov ali vrst dejanj obdelave, ki jih mora opraviti upravljavec za izvedbo pogodbe v smislu člena 6(1)(b)[17]. Te smernice obravnavajo tudi primere, ki lahko posameznike, na katere se nanašajo osebni podatki in ki jih morda zanima le ena od teh storitev, vodijo v položaj „vzemi ali pusti“. To se lahko zgodi, kadar želi upravljavec združiti več ločenih storitev ali delov storitve z različnimi temeljnimi nameni, lastnostmi ali razlogi v eno pogodbo. Če se pogodba nanaša na več ločenih storitev ali delov storitve, ki se lahko dejansko razumno izvedejo neodvisno druga od druge, bi bilo treba uporabo člena 6(1)(b) oceniti ločeno za vsako posamezno storitev, pri čemer bi bilo treba preveriti, kaj je objektivno potrebno za izvedbo vsake posamezne storitve, ki jo je posameznik, na katerega se nanašajo osebni podatki, aktivno zahteval ali se nanjo prijavil[18].

19. V skladu s temi smernicami morajo upravljavci oceniti, kaj je objektivno potrebno za izvajanje pogodbe. Če upravljavci ne morejo dokazati, da je obdelava osebnih podatkov plačilnega računa

[14] Smernice 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, Evropski odbor za varstvo podatkov, stran 8.
[15] Prav tam.
[16] Prav tam, stran 7.
[17] Prav tam, stran 10.
[18] Prav tam, stran 11.

objektivno potrebna za ločeno zagotavljanje vsake od zadevnih storitev, člen 6(1)(b) Splošne uredbe o varstvu podatkov ni veljavna pravna podlaga za obdelavo. V takih primerih bi moral upravljavec preučiti uporabo druge pravne podlage za obdelavo.

2.3 Preprečevanje goljufij

20. Člen 94(1) direktive PSD2 določa, da države članice dovolijo obdelavo osebnih podatkov v plačilnih sistemih in pri ponudnikih plačilnih storitev, ko je to potrebno za preprečevanje, preiskavo in odkrivanje plačilnih goljufij. Obdelava osebnih podatkov, nujno potrebna za preprečevanje zlorab, lahko pomeni zakoniti interes zadevnega ponudnika plačilnih storitev, kadar nad takimi interesi ne prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki[19]. Dejavnosti obdelave za namen preprečevanja zlorab bi morale temeljiti na upravljavčevi skrbni oceni vsakega posameznega primera v skladu z načelom odgovornosti. Poleg tega lahko za upravljavce za preprečevanje zlorab veljajo posebne pravne obveznosti, ki zahtevajo obdelavo osebnih podatkov.

2.4 Nadaljnja obdelava (ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil)

21. Člen 6(4) Splošne uredbe o varstvu podatkov določa pogoje za obdelavo osebnih podatkov za drug namen kot za tistega, za katerega so bili osebni podatki zbrani. Natančneje, taka nadaljnja obdelava se lahko opravi, kadar temelji na pravu Unije ali pravu države članice, ki pomeni potreben in sorazmeren ukrep v demokratični družbi za uresničevanje ciljev iz člena 23(1), kadar je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo ali kadar je obdelava za drug namen kot za tistega, za katerega so bili osebni podatki zbrani, skladna s prvotnim namenom.

22. Člena 66(3)(g) in 67(2)(f) direktive PSD2 je treba natančno upoštevati. Kot je že navedeno, člen 66(3)(g) direktive PSD2 določa, da ponudnik storitev odreditve plačil podatkov ne uporablja, ne dostopa do njih in jih ne hrani za druge namene kot za namene opravljanja storitve odreditve plačila, ki jo plačnik izrecno zahteva. Člen 67(2)(f) direktive PSD2 določa, da ponudnik storitev zagotavljanja informacij o računih podatkov ne uporablja, ne dostopa do njih ali jih ne hrani za druge namene kot za namene opravljanja storitve zagotavljanja informacij o računih, ki jo uporabnik plačilnih storitev izrecno zahteva v skladu s predpisi o varstvu podatkov.

23. Posledično člena 66(3)(g) in 67(2)(f) direktive PSD2 močno omejujeta možnosti obdelave za druge namene, kar pomeni, da obdelava za drug namen ni dovoljena, razen če je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo v skladu s členom 6(1)(a) Splošne uredbe o varstvu podatkov ali pa obdelava v skladu s členom 6(4) Splošne uredbe o varstvu podatkov temelji na pravu Unije ali pravu države članice, ki velja za upravljavca. Kadar obdelava podatkov za drug namen kot za tistega, za katerega so bili osebni podatki zbrani, ne temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki, ali na pravu Unije ali pravu države članice, omejitve iz členov 66(3)(g) in 67(2)(f) direktive PSD2 jasno določajo, da noben drug namen ni združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani. Preskus združljivosti člena 6(4) Splošne uredbe o varstvu podatkov ne more prinesti pravne podlage za obdelavo.

24. Člen 6(4) Splošne uredbe o varstvu podatkov omogoča nadaljnjo obdelavo na podlagi prava Unije ali prava države članice. Vsi ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih so na primer pooblaščeni subjekti iz člena 3(2)(a) Direktive (EU) 2015/849 Evropskega parlamenta in Sveta z dne 20. maja 2015 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma (direktiva o preprečevanju pranja denarja). Ti

[19] Uvodna izjava 47 Splošne uredbe o varstvu podatkov.

pooblaščeni subjekti morajo torej uporabiti ukrepe skrbnega preverjanja strank, kot določa Direktiva. Osebni podatki, obdelani v povezavi s storitvijo iz direktive PSD2, se torej nadalje obdelajo na podlagi najmanj ene pravne obveznosti, ki jo ima ponudnik storitev[20].

25. Kot je omenjeno v odstavku 20, člen 6(4) Splošne uredbe o varstvu podatkov določa, da lahko obdelava za drug namen kot za tistega, za katerega so bili osebni podatki zbrani, temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki, če so izpolnjeni vsi pogoji za privolitev iz Splošne uredbe o varstvu podatkov. Kot je navedeno zgoraj, mora upravljavec dokazati, da je privolitev mogoče zavrniti ali preklicati brez škode (uvodna izjava 42 Splošne uredbe o varstvu podatkov).

2.5 Zakonit razlog za omogočanje dostopa do računa (ponudniki plačilnih storitev, ki vodijo račune)

26. Kot je že omenjeno v odstavku 10, lahko uporabniki plačilnih storitev uveljavljajo pravico do uporabe storitev odreditve plačil in storitev zagotavljanja informacij o računih. Obveznosti, ki ju državam članicam nalagata člena 66(1) in 67(1) direktive PSD2, bi bilo treba prenesti v nacionalno pravo, da se zagotovi učinkovita uporaba pravice uporabnika plačilnih storitev pri koriščenju omenjenih plačilnih storitev. Učinkovita uporaba takih pravic ne bi bila mogoča brez ustreznih obveznosti ponudnika plačilnih storitev, ki vodi račun, običajno je to banka, da ponudniku plačilnih storitev omogoči dostop do računa pod pogojem, da je izpolnil vse zahteve za dostop do računa uporabnika plačilnih storitev. Poleg tega člena 66(5) in 67(4) direktive PSD2 jasno določata, da opravljanje storitev odreditve plačil in opravljanje storitev zagotavljanja informacij o računih ni pogojeno z obstojem pogodbenega razmerja med ponudniki storitev odreditve plačil oziroma ponudniki storitev zagotavljanja informacij o računih ter ponudniki plačilnih storitev, ki vodijo račune.

27. Obdelava osebnih podatkov s strani ponudnika plačilnih storitev, ki vodi račune, ki je sestavljena iz omogočanja dostopa do osebnih podatkov, ki ga zahtevata ponudnik storitev odreditve plačil in ponudnik storitev zagotavljanja informacij o računih, da lahko opravljata plačilne storitve za uporabnika plačilnih storitev, temelji na pravni obveznosti. Za doseganje teh ciljev direktive PSD2 morajo ponudniki plačilnih storitev, ki vodijo račune, za storitve ponudnikov storitev odreditve plačil in ponudnikov storitev zagotavljanja informacij o računih zagotoviti osebne podatke, kar je za ponudnike storitev odreditve plačil in ponudnike storitev zagotavljanja informacij o računih nujen pogoj za opravljanje storitev ter s tem za zagotavljanje pravic iz členov 66(1) in 67(1) direktive PSD2. Zato je veljavna pravna podlaga v tem primeru člen 6(1)(c) Splošne uredbe o varstvu podatkov.

28. Ker Splošna uredba o varstvu podatkov določa, da mora biti obdelava na podlagi pravne obveznosti jasno določena v skladu s pravom Unije ali pravom države članice (glej člen 6(3) Splošne uredbe o varstvu podatkov), bi morala obveznost ponudnikov plačilnih storitev, ki vodijo račune, pri omogočanju dostopa izhajati iz nacionalnega prava, s katerim se prenese direktiva PSD2.

[20] Upoštevati je treba, da temeljito preverjanje vprašanja, ali direktiva o preprečevanju pranja denarja izpolnjuje standarde iz člena 6(4) Splošne uredbe o varstvu podatkov, ne spada na področje uporabe tega dokumenta.

3 IZRECNA PRIVOLITEV OZIROMA SOGLASJE

3.1 Privolitev v skladu s Splošno uredbo o varstvu podatkov

29. V skladu s Splošno uredbo o varstvu podatkov je privolitev ena od šestih pravnih podlag za zakonitost obdelave osebnih podatkov. Člen 4(11) Splošne uredbe o varstvu podatkov privolitev opredeljuje kot „vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali jasnega pritrdilnega dejanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katerim izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj“. Ti štirje pogoji, tj. prostovoljno, konkretno, informirano in nedvoumno, so bistveni za veljavnost privolitve. V skladu s Smernicami Evropskega odbora za varstvo podatkov št. 05/2020 o privolitvi na podlagi Uredbe 2016/679 je lahko privolitev ustrezna zakonita podlaga le, če sta posamezniku, na katerega se nanašajo osebni podatki, zagotovljena nadzor ter dejanska izbira med sprejetjem in zavrnitvijo pogojev ali njihova zavrnitev brez škode. Kadar upravljavec zaprosi za privolitev, mora oceniti, ali bo izpolnjeval vse zahteve za pridobitev veljavne privolitve. Če je privolitev pridobljena popolnoma v skladu s Splošno uredbo o varstvu podatkov, je orodje, ki posameznikom, na katere se nanašajo osebni podatki, omogoča nadzor nad tem, ali bodo osebni podatki v zvezi z njimi obdelani ali ne. Če ni, nadzor posameznikov, na katere se nanašajo osebni podatki, postane navidezen, privolitev pa bo neveljavna pravna podlaga za obdelavo, zaradi česar bo dejavnost obdelave nezakonita[21].

30. Splošna uredba o varstvu podatkov vsebuje tudi nadaljnje zaščitne ukrepe v členu 7, ki določa, da mora biti upravljavec zmožen dokazati obstoj veljavne privolitve v času obdelave. Prav tako mora biti zahteva za privolitev predložena na način, ki se jasno razlikuje od drugih zadev, v razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Poleg tega mora biti posameznik, na katerega se nanašajo osebni podatki, obveščen o pravici, da svojo privolitev kadar koli prekliče, pri čemer je privolitev enako enostavno preklicati kot dati.

31. V skladu s členom 9 Splošne uredbe o varstvu podatkov je privolitev ena od izjem od splošne prepovedi obdelave posebnih vrst osebnih podatkov. Vendar mora biti v takem primeru privolitev posameznika, na katerega se nanašajo osebni podatki, „izrecna“[22].

32. V skladu s Smernicami Evropskega odbora za varstvo podatkov št. 05/2020 o privolitvi na podlagi Uredbe 2016/679 se izrecna privolitev iz Splošne uredbe o varstvu podatkov nanaša na način, kako posameznik, na katerega se nanašajo osebni podatki, izrazi privolitev. To pomeni, da bi moral posameznik, na katerega se nanašajo osebni podatki, dati izrecno izjavo o privolitvi za določen(-a) namen(-e) obdelave. Očiten način za zagotovitev, da je privolitev izrecna, bi bil, da se privolitev izrecno potrdi v pisni izjavi. Upravljavec bi lahko, kjer je to ustrezno, poskrbel, da posameznik, na katerega se nanašajo osebni podatki, podpiše pisno izjavo, da se odpravijo vsi mogoči dvomi in morebitno pomanjkanje dokazov v prihodnosti.

33. V nobenem primeru za privolitev ni mogoče šteti morebitnih dvoumnih izjav ali dejanj. Upravljavec mora tudi paziti, da privolitve ni mogoče pridobiti z istim dejanjem, kot je potrebno za sprejetje pogodbe ali strinjanje s splošnimi pogoji storitve.

3.2 Soglasje v skladu z direktivo PSD2

[21] Smernice št. 05/2020 o privolitvi na podlagi Uredbe 2016/679, Evropski odbor za varstvo podatkov, odstavek 3.

[22] Glej tudi Mnenje št. 15/2011 o opredelitvi privolitve (WP 187), stran 6–8, in/ali Mnenje št. 6/2014 o pojmu zakonitih interesov upravljavca podatkov iz člena 7 Direktive 95/46/ES (WP 217), stran 9, 10, 13 in 14.

34. Evropski odbor za varstvo podatkov upošteva, da je pravni okvir glede izrecnega soglasja kompleksen, saj koncept „izrecnega soglasja oziroma privolitve“ vključujeta tako direktiva PSD2 kot tudi Splošna uredba o varstvu podatkov. To sproža vprašanje, ali naj se „izrecno soglasje“, kot ga omenja člen 94(2) direktive PSD2, razlaga enako kot izrecna privolitev iz Splošne uredbe o varstvu podatkov.

3.2.1 Izrecno soglasje iz člena 94(2) direktive PSD2

35. Direktiva PSD2 vključuje več posebnih pravil glede obdelave osebnih podatkov, zlasti v členu 94(1), ki določa, da mora biti obdelava osebnih podatkov za namene direktive PSD2 skladna s pravom EU o varstvu podatkov. Poleg tega člen 94(2) direktive PSD2 določa, da ponudniki plačilnih storitev dostopajo le do tistih osebnih podatkov, ki so potrebni za opravljanje njihovih plačilnih storitev, ter jih obdelujejo in hranijo z izrecnim soglasjem uporabnika plačilnih storitev. V skladu s členom 33(2) direktive PSD2 ta zahteva za izrecno soglasje uporabnika plačilnih storitev ne velja za ponudnike storitev zagotavljanja informacij o računih. Vendar člen 67(2)(a) direktive PSD2 za opravljanje storitve še vedno določa izrecno soglasje za ponudnike storitev zagotavljanja informacij o računih.

36. Kot je navedeno zgoraj, je seznam zakonitih podlag za obdelavo v skladu s Splošno uredbo o varstvu podatkov izčrpen. Kot je navedeno v odstavku 14, je pravna podlaga za obdelavo osebnih podatkov za opravljanje plačilnih storitev načeloma člen 6(1)(b) Splošne uredbe o varstvu podatkov, kar pomeni, da je obdelava potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe. Iz tega izhaja, da člena 94(2) direktive PSD2 ni mogoče obravnavati kot dodatno pravno podlago za obdelavo osebnih podatkov. Evropski odbor za varstvo podatkov meni, da bi bilo treba ta odstavek glede na navedeno razlagati po eni strani v skladu z veljavnim pravnim okvirom za varstvo podatkov in po drugi strani na način, ki ohranja njegov koristen učinek. Izrecno soglasje iz člena 94(2) direktive PSD2 bi bilo torej treba šteti za dodatno zahtevo pogodbene narave[23] v zvezi z dostopom do osebnih podatkov ter njihovo posledično obdelavo in hrambo za namene opravljanja plačilnih storitev ter torej ni enako (izrecni) privolitvi iz Splošne uredbe o varstvu podatkov.

37. „Izrecno soglasje“ iz člena 94(2) direktive PSD2 je pogodbeno soglasje. To pomeni, da bi bilo treba člen 94(2) direktive PSD2 razlagati v smislu, da morajo biti posamezniki, na katere se nanašajo osebni podatki, ob sklenitvi pogodbe s ponudnikom plačilnih storitev v skladu z direktivo PSD2 v celoti seznanjeni s posebnimi vrstami osebnih podatkov, ki se bodo obdelovali. Nadalje morajo biti seznanjeni s posebnim namenom (plačilne storitve), za katerega se bodo njihovi osebni podatki obdelovali, in se morajo s temi določili izrecno strinjati. Taka določila bi se morala jasno razlikovati od drugih zadev, obravnavanih v pogodbi, in bi jih moral posameznik, na katerega se osebni podatki nanašajo, izrecno sprejeti.

38. Bistveno pri pojmu „izrecno soglasje“ iz člena 94(2) direktive PSD2 je pridobitev dostopa do osebnih podatkov za posledično obdelavo in hrambo teh podatkov za namen opravljanja plačilnih storitev. To pomeni, da ponudnik plačilnih storitev[24] osebnih podatkov še ne obdeluje, potrebuje pa dostop do osebnih podatkov, ki se obdelujejo pod odgovornostjo katerega koli drugega upravljavca. Če uporabnik plačilnih storitev sklene pogodbo na primer s ponudnikom storitev odreditve plačil, mora ta ponudnik pridobiti dostop do osebnih podatkov uporabnika plačilnih storitev, ki se obdelujejo pod odgovornostjo ponudnika plačilnih storitev, ki vodi račun. Predmet

[23] Dopis Evropskega odbora za varstvo podatkov v zvezi z direktivo PSD2, 5. julij 2018, stran 4.
[24] To velja za storitve od 1 do 7 v Prilogi I k direktivi PSD2.

izrecnega soglasja iz člena 94(2) direktive PSD2 je dovoljenje za pridobitev dostopa do navedenih osebnih podatkov, tako da je mogoče obdelovati in hraniti tiste osebne podatke, ki so potrebni za opravljanje plačilnih storitev. Če posameznik, na katerega se nanašajo osebni podatki, da izrecno soglasje, mora ponudnik plačilnih storitev, ki vodi račun, omogočiti dostop do navedenih osebnih podatkov.

39. Čeprav soglasje iz člena 94(2) direktive PSD2 ni pravna podlaga za obdelavo osebnih podatkov, se to soglasje posebej nanaša na osebne podatke in varstvo podatkov ter zagotavlja preglednost in stopnjo nadzora za uporabnika plačilnih storitev[25]. Direktiva PSD2 sicer ne določa podrobno vsebinskih pogojev za soglasje iz člena 94(2) direktive PSD2, vendar pa bi ga bilo treba, kot je navedeno zgoraj, razumeti v skladu z veljavnim pravnim okvirom za varstvo podatkov in na način, ki ohranja njegov koristen učinek.

40. Glede informacij, ki jih morajo zagotoviti upravljavci, in zahteve po preglednosti smernice Delovne skupine iz člena 29 o preglednosti določajo, da je „[o]srednji element načela preglednosti, določenega v teh določbah, […] zmožnost posameznika, na katerega se nanašajo osebni podatki, da vnaprej ugotovi obseg in posledice obdelave, pri čemer ga pozneje ne bi smeli presenetiti načini, kako so se njegovi osebni podatki uporabili“[26].

41. Poleg tega, kot zahteva načelo omejitve namena, je treba osebne podatke zbirati za določene, izrecne in zakonite namene (člen 5(1)(b) Splošne uredbe o varstvu podatkov). Če se osebni podatki zbirajo za več namenov, „bi se morali upravljavci izogniti opredelitvi le enega širšega namena za utemeljitev različnih dejavnosti nadaljnje obdelave, ki so dejansko le malo povezane z dejanskim prvotnim namenom“[27]. Evropski odbor za varstvo podatkov je poudaril, nazadnje v kontekstu pogodb za spletne storitve, tveganje vključitve splošnih pogojev obdelave v pogodbe ter navedel, da bi moral biti namen zbiranja jasno in določno opredeljen: moral bi biti dovolj podroben, da se ugotovi, katera vrsta obdelave je vključena v navedeni namen in katera ni vključena, ter da se omogočita ocena skladnosti z zakonodajo in uporaba zaščitnih ukrepov za varstvo podatkov[28].

42. V okviru konteksta dodatne zahteve po izrecnem soglasju v skladu s členom 94(2) direktive PSD2 to pomeni, da morajo upravljavci posameznikom, na katere se nanašajo osebni podatki, zagotoviti specifične in izrecne informacije o posebnih namenih, ki jih je opredelil upravljavec ter za katere se do osebnih podatkov dostopa in se osebni podatki obdelujejo in hranijo. Skladno s členom 94(2) direktive PSD2 morajo posamezniki, na katere se osebni podatki nanašajo, te posebne namene izrecno sprejeti.

43. Poleg tega Evropski odbor za varstvo podatkov poudarja, kot je navedeno v odstavku 10, da mora imeti uporabnik plačilnih storitev možnost izbire, ali želi uporabiti storitev ali ne, in ga v to ni mogoče prisiliti. Zato mora biti soglasje iz člena 94(2) direktive PSD2 prav tako prostovoljno.

3.3 Sklep

44. Izrecno soglasje iz direktive PSD2 se razlikuje od (izrecne) privolitve iz Splošne uredbe o varstvu podatkov. Izrecno soglasje iz člena 94(2) direktive PSD2 je dodatna pogodbena zahteva. Ko mora

[25] Člen 94(2) direktive PSD2 spada v poglavje 4 „Varstvo podatkov“.
[26] Delovna skupina iz člena 29, Smernice o preglednosti na podlagi Uredbe (EU) 2016/679, odstavek 10 (sprejete 11. aprila 2018), ki jih je potrdil Evropski odbor za varstvo podatkov.
[27] Mnenje Delovne skupine iz člena 29 št. 3/2013 o omejitvi namena (WP 203), stran 16.
[28] Smernice 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, odstavek 16 (različica za javno posvetovanje), in Mnenje Delovne skupine iz člena 29 št. 3/2013 o omejitvi namena (WP 203), strani 15–16.

ponudnik plačilnih storitev za opravljanje plačilne storitve dostopati do osebnih podatkov, je potrebno izrecno soglasje uporabnika plačilnih storitev v skladu s členom 94(2) direktive PSD2.

4 OBDELAVA PODATKOV TIHE STRANKE

4.1 Podatki tihe stranke

45. Vprašanje varstva podatkov, ki zahteva skrben premislek, je obdelava tako imenovanih „podatkov tihe stranke“. V kontekstu tega dokumenta so podatki tihe stranke osebni podatki, ki zadevajo posameznika, na katerega se nanašajo, ki ni uporabnik posameznega ponudnika plačilnih storitev, vendar pa zadevni ponudnik plačilnih storitev obdeluje njegove osebne podatke za izvajanje pogodbe med ponudnikom in uporabnikom plačilnih storitev. Tako je na primer v primeru, ko uporabnik plačilnih storitev, posameznik A, na katerega se nanašajo osebni podatki, koristi storitve ponudnika storitev zagotavljanja informacij o računih, posameznik B, na katerega se osebni podatki nanašajo, pa je na plačilni račun posameznika A izvedel več plačilnih transakcij. V tem primeru je posameznik B „tiha stranka“, osebni podatki (kot sta številka računa posameznika B in znesek izvedenih transakcij) v zvezi s posameznikom B pa so „podatki tihe stranke“.

4.2 Zakoniti interes upravljavca

46. Člen 5(1)(b) Splošne uredbe o varstvu podatkov določa, da se osebni podatki zbirajo le za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni. Poleg tega Splošna uredba o varstvu podatkov določa, da mora biti vsakršna obdelava osebnih podatkov potrebna in sorazmerna ter v skladu z načeli varstva podatkov, na primer z načelom omejitve namena in načelom najmanjšega obsega podatkov.

47. Splošna uredba o varstvu podatkov lahko dovoljuje obdelavo podatkov tihe stranke, kadar je taka obdelava potrebna za namene zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba (člen 6(1)(f) Splošne uredbe o varstvu podatkov). Vendar pa lahko taka obdelava poteka le, kadar nad zakonitimi interesi upravljavca ne „prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov“.

48. Zakonita podlaga za obdelavo podatkov tihe stranke s strani ponudnikov storitev odreditve plačil in ponudnikov storitev zagotavljanja informacij o računih – v okviru opravljanja plačilnih storitev v skladu z direktivo PSD2 – bi tako lahko bil zakoniti interes upravljavca ali tretje osebe, da izvaja pogodbo, sklenjeno z uporabnikom plačilnih storitev. Potrebnost obdelave osebnih podatkov tihe stranke je omejena in določena z razumnimi pričakovanji zadevnih posameznikov, na katere se nanašajo osebni podatki. V okviru opravljanja plačilnih storitev, ki jih zajema direktiva PSD2, je treba vzpostaviti učinkovite in ustrezne ukrepe za zagotovitev, da nad interesi ali temeljnimi pravicami in svoboščinami tihih strank ne bodo prevladali drugi interesi, ter zagotovitev, da se upoštevajo razumna pričakovanja navedenih posameznikov, na katere se nanašajo osebni podatki, glede obdelave njihovih osebnih podatkov. Glede tega mora upravljavec (ponudnik storitev zagotavljanja informacij o računih ali ponudnik storitev odreditve plačil) vzpostaviti potrebne zaščitne ukrepe za obdelavo, da se zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki. To vključuje tehnične ukrepe za zagotovitev, da se podatki tihe stranke ne obdelujejo za drug namen kot za tistega, za katerega so ponudniki storitev odreditve plačil in ponudniki storitev zagotavljanja informacij o računih prvotno zbirali osebne podatke. Če je izvedljivo, bi bilo treba uporabiti tudi šifriranje ali druge tehnike, da se dosežeta ustrezna raven varnosti in najmanjši obseg podatkov.

4.3 Nadaljnja obdelava osebnih podatkov tihe stranke

49. Kot je navedeno v odstavku 29, je mogoče osebne podatke, ki se obdelujejo v zvezi s plačilno storitvijo, ki jo ureja direktiva PSD2, nadalje obdelovati na podlagi pravnih obveznosti, ki jih ima ponudnik storitve. Te pravne obveznosti bi lahko zadevale osebne podatke tihe stranke.

50. Evropski odbor za varstvo podatkov glede nadaljnje obdelave podatkov tihe stranke na podlagi zakonitega interesa meni, da takih podatkov ni mogoče uporabiti za drug namen kot za tistega, za katerega so se osebni podatki zbirali, razen na podlagi prava EU ali prava države članice. Privolitev tihe stranke pravno ni izvedljiva, kajti za pridobitev privolitve bi se morali osebni podatki tihe stranke zbirati ali obdelovati, za to pa v členu 6 Splošne uredbe o varstvu podatkov ni pravne podlage. Tudi preskus združljivosti iz člena 6(4) Splošne uredbe o varstvu podatkov ne more zagotoviti podlage za obdelavo za druge namene (na primer dejavnosti neposrednega trženja). Pravice in svoboščine takih posameznikov, na katere se nanašajo podatki tihe stranke, ne bodo spoštovane, če nov upravljavec podatkov osebne podatke uporablja za druge namene, ob upoštevanju okoliščin, v katerih so se osebni podatki zbirali, zlasti neobstoja kakršnega koli razmerja s posamezniki, na katere se nanašajo osebni podatki, ki so tihe stranke[29], neobstoja kakršne koli povezave med katerim koli drugim namenom in namenom, za katerega so se osebni podatki prvotno zbirali (tj. dejstvo, da ponudniki plačilnih storitev podatke tihe stranke potrebujejo le za izvajanje pogodbe, sklenjene z drugo pogodbeno stranko), narave zadevnih osebnih podatkov[30], okoliščine, da posamezniki, na katere se nanašajo osebni podatki, ne morejo razumno pričakovati nadaljnje obdelave ali celo biti seznanjeni s tem, kateri upravljavec morda obdeluje njihove osebne podatke, ter pravnih omejitev obdelave iz členov 66(3)(g) in 67(2)(f) direktive PSD2.

[29] V uvodni izjavi 87 direktive PSD2 je navedeno, da se direktiva PSD2 nanaša le na „pogodbene obveznosti in odgovornosti med uporabnikom plačilnih storitev in ponudnikom plačilnih storitev“. Podatki tihe stranke torej ne spadajo v področje uporabe direktive PSD2.

[30] Posebno pozornost bi bilo treba nameniti obdelavi osebnih finančnih podatkov, saj se lahko v skladu s smernicami glede ocene učinka glede varstva podatkov za obdelavo šteje, da povečuje možno tveganje za pravice in svoboščine posameznikov.

5 OBDELAVA POSEBNIH VRST OSEBNIH PODATKOV V SKLADU Z DIREKTIVO PSD2

5.1 Posebne vrste osebnih podatkov

51. Člen 9(1) Splošne uredbe o varstvu podatkov prepoveduje obdelavo „osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelav[o] genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo“.

52. Treba je poudariti, da so v nekaterih državah članicah elektronska plačila že zelo razširjena in jih v vsakodnevnih transakcijah marsikdo uporablja raje kot gotovino. Hkrati lahko finančne transakcije o posamezniku, na katerega se nanašajo osebni podatki, razkrijejo občutljive informacije, tudi informacije, povezane s posebnimi vrstami osebnih podatkov. Na podlagi podrobnosti o transakcijah je na primer mogoče iz donacij političnim strankam ali organizacijam, cerkvam ali župnijam razbrati politična in verska prepričanja. Članstvo v sindikatu je mogoče razbrati iz nakazila letne članarine s posameznikovega bančnega računa. Osebne podatke v zvezi z zdravjem je mogoče zbirati na podlagi analize računov za zdravstvene storitve, ki jih je posameznik, na katerega se nanašajo osebni podatki, plačal zdravstvenemu delavcu (na primer psihiatru). Informacije o posameznih nakupih lahko razkrijejo informacije o spolnem življenju ali spolni usmerjenosti posameznika. Kot prikazujejo ti primeri, lahko že posamezne transakcije vsebujejo posebne vrste osebnih podatkov. Poleg tega se lahko storitve zagotavljanja informacij o računih opirajo na oblikovanje profilov, kot je opredeljeno v členu 4(4) Splošne uredbe o varstvu podatkov. Kot je navedeno v Smernicah Delovne skupine iz člena 29 o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, kot jih je potrdil Evropski odbor za varstvo podatkov, se lahko „[z] oblikovanjem profilov [...] podatki posebne vrste ustvarijo s sklepanjem iz podatkov, ki niso podatki posebne kategorije sami po sebi, ampak to postanejo v kombinaciji z drugimi podatki“[31]. To pomeni, da se lahko s seštevkom finančnih transakcij razkrijejo različni vedenjski vzorci, kar lahko vključuje posebne vrste osebnih podatkov. Zato obstajajo velike možnosti, da ponudnik storitev, ki obdeluje informacije o finančnih transakcijah posameznikov, na katere se nanašajo osebni podatki, obdeluje tudi posebne vrste osebnih podatkov.

53. Evropski odbor za varstvo podatkov glede pojma „občutljivi plačilni podatki“ ugotavlja naslednje: opredelitev občutljivih plačilnih podatkov v direktivi PSD2 se precej razlikuje od načina, kako se pojem „občutljivi osebni podatki“ na splošno uporablja v okviru Splošne uredbe o varstvu podatkov in v okviru varstva podatkov (pravu o varstvu podatkov). Direktiva PSD2 „občutljive plačilne podatke“ opredeljuje kot „podatke, vključno z osebnimi varnostnimi elementi, ki se lahko uporabijo za goljufijo“, Splošna uredba o varstvu podatkov pa poudarja potrebo po posebnem varstvu posebnih vrst osebnih podatkov, ki so v skladu z njenim členom 9 po svoji naravi posebej občutljivi z vidika temeljnih pravic in svoboščin, kot so posebne vrste osebnih podatkov[32]. Glede tega se priporočata vsaj natančnejša opredelitev in kategorizacija vrst osebnih podatkov, ki se bodo obdelovali. Verjetno bo potrebna ocena učinka v zvezi z varstvom podatkov v skladu s členom 35 Splošne uredbe o varstvu podatkov, ki bo pripomogla k natančnejši opredelitvi. Več navodil glede ocen učinka v zvezi z varstvom podatkov je na voljo v Smernicah Delovne skupine iz člena 29 glede

[31] Delovna skupina za varstvo podatkov iz člena 29, Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, WP 251 rev. 01, stran 15.
[32] Na primer, v uvodni izjavi 10 Splošne uredbe o varstvu podatkov so posebne vrste osebnih podatkov „občutljivi podatki“.

ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, kot jih je potrdil Evropski odbor za varstvo podatkov.

5.2 Možna odstopanja

54. Prepoved iz člena 9 Splošne uredbe o varstvu podatkov ni absolutna. Odstopanj iz odstavkov (b) do (f) in (h) do (j) člena 9(2) Splošne uredbe o varstvu podatkov očitno ni mogoče uporabiti za obdelavo osebnih podatkov v kontekstu direktive PSD2, je pa zlasti mogoče upoštevati naslednji odstopanji iz člena 9(2) Splošne uredbe o varstvu podatkov:

a) prepoved se ne uporablja, če je posameznik, na katerega se nanašajo osebni podatki, dal izrecno privolitev v obdelavo navedenih osebnih podatkov za enega ali več določenih namenov (člen 9(2)(a) Splošne uredbe o varstvu podatkov);

b) prepoved se ne uporablja, če je obdelava potrebna iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava države članice, ki je sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki (člen 9(2)(g) Splošne uredbe o varstvu podatkov).

55. Poudariti je treba, da je seznam odstopanj v členu 9(2) Splošne uredbe o varstvu podatkov izčrpen. Ponudnik storitev mora prepoznati možnost, da so posebne vrste osebnih podatkov vključene v osebne podatke, ki se obdelujejo za opravljanje katere koli od storitev iz direktive PSD2. Ker za navedene ponudnike storitev velja prepoved iz člena 9(1) Splošne uredbe o varstvu podatkov, morajo ti zagotoviti, da zanje velja ena od izjem iz člena 9(2) Splošne uredbe o varstvu podatkov. Treba je poudariti, da se, kadar ponudnik storitev ne more dokazati izpolnjevanja pogojev enega od odstopanj, uporablja prepoved iz člena 9(1).

5.3 Bistven javni interes

56. Ponudniki plačilnih storitev lahko obdelujejo posebne vrste osebnih podatkov iz razlogov bistvenega javnega interesa, vendar le, če so izpolnjeni vsi pogoji iz člena 9(2)(g) Splošne uredbe o varstvu podatkov. To pomeni, da mora biti obdelava posebnih vrst osebnih podatkov obravnavana s posebnim odstopanjem od člena 9(1) Splošne uredbe o varstvu podatkov v pravu Unije ali pravu države članice. Ta določba bo morala obravnavati sorazmernost v zvezi s ciljem, za katerega se prizadeva z obdelavo, ter vsebovati ustrezne in specifične ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki. Poleg tega bo morala ta določba na podlagi prava Unije ali prava države članice spoštovati bistvo pravice do varstva podatkov. Treba je tudi dokazati, da je obdelava posebnih vrst podatkov potrebna iz razloga bistvenega javnega interesa, vključno s sistemsko pomembnimi interesi. To odstopanje bi bilo mogoče za nekatere vrste plačilnih storitev uporabiti šele, ko bi bili v celoti izpolnjeni vsi navedeni pogoji.

5.4 Izrecna privolitev

57. Kadar se odstopanje iz člena 9(2)(g) Splošne uredbe o varstvu podatkov ne uporablja, se zdi pridobitev izrecne privolitve v skladu s pogoji za veljavno privolitev iz Splošne uredbe za varstvo podatkov edino možno zakonito odstopanje za obdelavo posebnih vrst podatkov s strani tretjih ponudnikov storitev. Smernice Evropskega odbora za varstvo podatkov št. 05/2020 o privolitvi na podlagi Uredbe 2016/679 navajajo[33] naslednje: „Člen 9(2) ne priznava obdelave, ‚potrebne za

[33] Smernice št. 05/2020 o privolitvi na podlagi Uredbe 2016/679, Evropski odbor za varstvo podatkov, odstavek 99.

izvajanje pogodbe‘, kot izjeme od splošne prepovedi obdelave posebnih vrst podatkov. Zato bi morali upravljavci in države članice, ki obravnavajo ta položaj, preučiti posebne izjeme iz člena 9(2)(b) do (j).“ Ko ponudniki storitev uporabljajo člen 9(2)(a) Splošne uredbe o varstvu podatkov, morajo zagotoviti, da pred začetkom obdelave pridobijo izrecno privolitev. Izrecna privolitev, kot je določena v členu 9(2)(a) Splošne uredbe o varstvu podatkov, mora izpolnjevati vse zahteve Splošne uredbe o varstvu podatkov.

5.5 Ni ustreznega odstopanja

58. Kot je navedeno zgoraj, se, kadar ponudnik storitev ne more dokazati izpolnjevanja pogojev enega od odstopanj, uporablja prepoved iz člena 9(1). V tem primeru bi bilo mogoče vzpostaviti tehnične ukrepe za preprečitev obdelave posebnih vrst osebnih podatkov, na primer s preprečitvijo obdelave določenih podatkovnih točk. Glede tega lahko ponudniki plačilnih storitev raziščejo tehnične možnosti za izločitev posebnih vrst osebnih podatkov in omogočijo selektiven dostop, kar bi preprečilo, da bi tretji ponudniki storitev obdelovali posebne vrste osebnih podatkov tihih strank.

6 NAJMANJŠI OBSEG PODATKOV, VARNOST, PREGLEDNOST, ODGOVORNOST IN OBLIKOVANJE PROFILOV

6.1 Najmanjši obseg podatkov ter vgrajeno in privzeto varstvo podatkov

59. Načelo najmanjšega obsega podatkov je določeno v členu 5(1)(c) Splošne uredbe o varstvu podatkov: „Osebni podatki morajo biti […] ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo“. To pravzaprav pomeni, da upravljavci v skladu z načelom najmanjšega obsega podatkov ne bi smeli obdelovati več osebnih podatkov, kot je potrebno za doseganje zadevnega posebnega namena. Kot je poudarjeno v poglavju 2, sta količina in vrsta osebnih podatkov, potrebnih za opravljanje plačilne storitve, določeni s ciljem in sporazumno dogovorjenim pogodbenim namenom[34]. Najmanjši obseg podatkov se uporablja za vsako obdelavo (na primer za vsako zbirko osebnih podatkov, za vsak dostop do osebnih podatkov in zahtevo zanje). V Smernicah Evropskega odbora za varstvo podatkov št. 4/2019 o vgrajenem in privzetem varstvu podatkov iz člena 25 je navedeno, da so „obdelovalci in ponudniki tehnologije prav tako prepoznani kot ključni omogočevalci vgrajenega in privzetega varstva podatkov [ter] bi se morali zavedati tudi, da morajo upravljavci osebne podatke obdelovati le s sistemi in tehnologijami z vgrajenim varstvom podatkov[35]“.

60. Člen 25 Splošne uredbe o varstvu podatkov vsebuje obveznosti za uporabo vgrajenega in privzetega varstva podatkov. Te obveznosti so še zlasti pomembne za načelo najmanjšega obsega podatkov. Ta člen določa, da upravljavci tako v času določanja sredstev obdelave kot tudi v času same obdelave izvajajo ustrezne tehnične in organizacijske ukrepe, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, ter v obdelavo vključijo potrebne zaščitne ukrepe, da se izpolnijo zahteve Splošne uredbe o varstvu podatkov in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki. Upravljavec izvede ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi, da se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave. Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost. Taki ukrepi lahko vključujejo šifriranje, psevdonimizacijo in druge tehnične ukrepe.

61. Ko se uporablja obveznost iz člena 25 Splošne uredbe o varstvu podatkov, so najnovejši tehnološki razvoj, stroški izvajanja ter narava, obseg, okoliščine in nameni obdelave, pa tudi tveganja za pravice in svoboščine posameznikov, ki so povezana z obdelavo in se razlikujejo po verjetnosti in resnosti, elementi, ki jih je treba upoštevati. Nadaljnja pojasnila v zvezi s to obveznostjo so na voljo v omenjenih Smernicah Evropskega odbora za varstvo podatkov št. 4/2019 o vgrajenem in privzetem varstvu osebnih podatkov iz člena 25.

6.2 Ukrepi za najmanjši obseg podatkov

62. Tretji ponudniki storitev, ki za opravljanje zahtevanih storitev dostopajo do podatkov plačilnega računa, morajo upoštevati tudi načelo najmanjšega obsega podatkov in morajo zbirati le tiste osebne podatke, ki so potrebni za opravljanje posameznih plačilnih storitev, ki jih zahteva uporabnik plačilnih storitev. Načeloma bi moral biti dostop do osebnih podatkov omejen na to, kar je potrebno za opravljanje plačilnih storitev. Kot je razvidno iz poglavja 2, direktiva PSD2 od ponudnikov plačilnih storitev, ki vodijo račune, zahteva izmenjavo informacij uporabnika plačilnih

[34] Smernice 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, Evropski odbor za varstvo podatkov, odstavek 32.
[35] Smernice št. 4/2019 o vgrajenem in privzetem varstvu osebnih podatkov iz člena 25, stran 29.

storitev na zahtevo uporabnika plačilnih storitev, kadar želi uporabnik plačilnih storitev uporabiti storitev odreditve plačil ali storitev zagotavljanja informacij o računih.

63. Kadar za izvajanje pogodbe niso potrebni vsi podatki plačilnega računa, bi moral ponudnik storitev zagotavljanja informacij o računih pred zbiranjem podatkov izbrati relevantne vrste podatkov. Vrste podatkov, ki morda niso potrebni, lahko na primer vključujejo identiteto tihe stranke in značilnosti transakcije. Prav tako morda ni treba prikazati IBAN bančnega računa tihe stranke, razen če to zahteva pravo države članice ali pravo EU.

64. V zvezi s tem bi bilo mogoče preučiti možno uporabo tehničnih ukrepov, ki tretjim ponudnikom storitev omogočajo ali olajšujejo spoštovanje obveznosti dostopa do in pridobivanja le tistih osebnih podatkov, ki so potrebni za opravljanje njihovih storitev, v okviru izvajanja ustreznih politik za varstvo podatkov v skladu s členom 24(2) Splošne uredbe o varstvu podatkov. Glede tega Evropski odbor za varstvo podatkov priporoča uporabo digitalnih orodij, da se ponudnikom storitev zagotavljanja informacij o računih zagotovi podpora pri spoštovanju obveznosti zbiranja le tistih osebnih podatkov, ki so potrebni za namene, za katere se obdelujejo. Če ponudnik storitev za opravljanje svoje storitve na primer ne potrebuje značilnosti transakcije (v polju za opis v evidencah transakcije), bi lahko digitalno orodje za izbiro delovalo kot pripomoček, s katerim tretji ponudniki storitev to polje izključijo iz splošnih operacij obdelave, ki jih izvajajo.

Primer 2:

Podjetje HappyPayments, naš ponudnik storitev zagotavljanja informacij o računih iz primera 1, želi zagotoviti, da obdeluje le tiste osebne podatke plačilnega računa, ki zanimajo njegove uporabnike. Dostop do več podatkov plačilnega računa za opravljanje storitve ne bi bil potreben. Zato omogoči uporabnikom izbiro specifičnih vrst informacij, ki jih zanimajo.

Uporabnik A želi pregled svoje porabe v zadnjih dveh mesecih. Zato za oba svoja bančna računa, odprta pri dveh različnih ponudnikih plačilnih storitev, ki vodita račune, zaprosi za informacije o vseh transakcijah v zadnjih dveh mesecih, o zneskih transakcij, o datumih izvršitev in imenu prejemnikov ter označi ustrezna polja v uporabniškem vmesniku podjetja HappyPayments.

Podjetje HappyPayments nato od zadevnih ponudnikov plačilnih storitev, ki vodita račune, zahteva le informacije, ki ustrezajo poljem, ki jih je uporabnik A označil, in le za obdobje zadnjih dveh mesecev. Informacij, kot sta na primer „namen“ prenosa ali celo IBAN, ne zahteva, saj uporabnik A zanje ni zaprosil.

Da bi podjetje HappyPayments lahko izpolnilo svoje obveznosti najmanjšega obsega podatkov, mu ponudnika plačilnih storitev, ki vodita račune, omogočita, da zahteva določena polja za razpon datumov.

65. Glede tega je treba tudi opozoriti, da smejo ponudniki plačilnih storitev, ki vodijo račune, v skladu z direktivo PSD2 omogočiti le dostop do informacij o plačilnem računu. V direktivi PSD2 ni pravne podlage za omogočanje dostopa do osebnih podatkov, vsebovanih v drugih računih, kot so varčevalni računi, hipoteke ali naložbeni računi. Zato je treba v skladu z direktivo PSD2 vzpostaviti tehnične ukrepe za zagotovitev, da je dostop omejen le na potrebne informacije o plačilnem računu.

66. Poleg tega, da mora ponudnik storitev zbrati čim manj podatkov, mora zagotoviti tudi omejena obdobja hrambe. Ponudnik storitev osebnih podatkov ne bi smel hraniti dlje, kot je potrebno glede na namene, ki jih zahteva uporabnik plačilnih storitev.

67. Če pogodba, sklenjena med posameznikom, na katerega se nanašajo osebni podatki, in ponudnikom storitev zagotavljanja informacij o računih, zahteva posredovanje osebnih podatkov

tretjim stranem, se lahko posredujejo le tisti osebni podatki, ki so potrebni za izvajanje pogodbe. Posamezniki, na katere se nanašajo osebni podatki, bi morali biti tudi posebej obveščeni o posredovanju in osebnih podatkih, ki bodo posredovani navedeni tretji strani.

6.3 Varnost

68. Evropski odbor za varstvo podatkov je že poudaril, da ima kršitev varstva osebnih finančnih podatkov „očitno resne posledice za vsakodnevno življenje posameznika, na katerega se nanašajo osebni podatki“, in kot primer navaja tveganja goljufije v zvezi s plačili[36].

69. Kadar kršitev varstva podatkov vključuje finančne podatke, je lahko posameznik, na katerega se nanašajo osebni podatki, izpostavljen znatnim tveganjem. Glede na razkrite informacije so lahko posamezniki, na katere se nanašajo osebni podatki, izpostavljeni tveganju kraje identitete ali kraje sredstev z njihovih računov in drugega premoženja. Poleg tega obstaja možnost, da je izpostavljenost podatkov o transakcijah povezana s precejšnjimi tveganji v zvezi z zasebnostjo, saj lahko podatki o transakciji vsebujejo navedbe o vseh vidikih zasebnega življenja posameznika, na katerega se nanašajo osebni podatki. Hkrati so finančni podatki seveda dragoceni za storilce kaznivih dejanj in so torej privlačna tarča.

70. Ponudniki plačilnih storitev so kot upravljavci obvezani sprejeti ustrezne ukrepe za varstvo osebnih podatkov posameznikov, na katere se osebni podatki nanašajo (člen 24(1) Splošne uredbe o varstvu podatkov). Večja kot so tveganja, povezana z dejavnostjo obdelave, ki jo izvaja upravljavec, višji so varnostni standardi, ki jih je treba uporabiti. Ker je obdelava finančnih podatkov povezana z različnimi resnimi tveganji, bi morali biti varnostni ukrepi ustrezno strogi.

71. Ponudniki storitev bi morali izpolnjevati visoke standarde, vključno z močnimi mehanizmi za avtentikacijo strank in visokimi varnostnimi standardi za tehnično opremo[37]. Pomembni so tudi drugi postopki, kot sta varnostno preverjanje obdelovalcev glede varnostnih standardov in izvajanje postopkov za preprečitev nedovoljenega dostopa.

6.4 Preglednost in odgovornost

72. Preglednost in odgovornost sta temeljni načeli Splošne uredbe o varstvu podatkov.

73. Glede preglednosti (člen 5(1)(a) Splošne uredbe o varstvu podatkov) člen 12 Splošne uredbe o varstvu podatkov določa, da upravljavci sprejmejo ustrezne ukrepe za zagotovitev vseh informacij iz členov 13 in 14 Splošne uredbe o varstvu podatkov. Poleg tega določa, da morajo biti informacije ali sporočila o obdelavi osebnih podatkov v jedrnati, pregledni, razumljivi in lahko dostopni obliki. Informacije morajo biti v jasnem in preprostem jeziku ter posredovane v pisni obliki „ali z drugimi sredstvi, vključno, kjer je ustrezno, z elektronskimi sredstvi“. Smernice Delovne skupine iz člena 29 o preglednosti na podlagi Uredbe (EU) 2016/679, kot jih je potrdil Evropski odbor za varstvo podatkov, zagotavljajo posebna navodila za skladnost z načelom preglednosti v digitalnih okoljih.

74. V skladu z omenjenimi Smernicami o preglednosti na podlagi Uredbe (EU) 2016/679 bi bilo treba člen 11 Splošne uredbe o varstvu podatkov razlagati kot način uveljavljanja dejanskega najmanjšega obsega podatkov, pri čemer se ne ovira uresničevanja pravic posameznika, na katerega se nanašajo osebni podatki, ter da bi moralo biti uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, omogočeno z dodatnimi informacijami, ki jih zagotovi

[36] Smernice Delovne skupine iz člena 29 glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, WP 248 rev. 01, ki jih je potrdil Evropski odbor za varstvo podatkov.
[37] Glej RTS.

posameznik, na katerega se nanašajo osebni podatki. Zgodi se lahko, da upravljavec podatkov obdeluje osebne podatke, pri čemer pa identifikacija posameznika, na katerega se nanašajo osebni podatki, ni potrebna (na primer s psevdonimiziranimi podatki). V takih primerih je lahko ustrezen tudi člen 11(1), saj določa, da upravljavec podatkov ni zavezan ohraniti, pridobiti ali obdelati dodatnih informacij, da bi identificiral posameznika, na katerega se nanašajo osebni podatki, samo zaradi zagotavljanja skladnosti s Splošno uredbo o varstvu podatkov.

75. Za storitve v okviru direktive PSD2 se člen 13 Splošne uredbe o varstvu podatkov uporablja za osebne podatke, pridobljene od posameznika, na katerega se ti podatki nanašajo, člen 14 pa se uporablja, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se ti nanašajo.

76. Posameznik, na katerega se nanašajo osebni podatki, mora biti zlasti obveščen o obdobju hrambe osebnih podatkov ali, če to ni mogoče, o merilih, s katerimi se tako obdobje določi, ter, kjer je primerno, o zakonitih interesih, za katere si prizadeva upravljavec ali morebitna tretja stran. Če obdelava temelji na privolitvi iz člena 6(1)(a) Splošne uredbe o varstvu podatkov ali na izrecni privolitvi iz člena 9(2)(a) Splošne uredbe o varstvu podatkov, mora biti posameznik, na katerega se nanašajo osebni podatki, obveščen o obstoju pravice, da se lahko privolitev kadar koli prekliče.

77. Informacije posamezniku, na katerega se nanašajo osebni podatki, zagotovi upravljavec ob upoštevanju posebnih okoliščin, v katerih se osebni podatki obdelujejo. Če se bodo osebni podatki uporabili za komuniciranje s posameznikom, na katerega se nanašajo osebni podatki[38], kar bo verjetno veljalo za ponudnike storitev zagotavljanja informacij o računih, je treba informacije zagotoviti najpozneje ob prvem komuniciranju s tem posameznikom. Če bodo osebni podatki razkriti drugemu uporabniku, je treba informacije zagotoviti najpozneje ob prvem razkritju osebnih podatkov.

78. Glede spletnih plačilnih storitev omenjene smernice pojasnjujejo, da lahko upravljavci podatkov uporabijo večdelni pristop, kadar se odločijo za uporabo kombinacije načinov za zagotavljanje preglednosti. Priporoča se zlasti, naj se večdelne izjave o varstvu osebnih podatkov uporabijo, da bi zagotovile povezave na različne vrste informacij, ki jih je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki, namesto da bi bile vse take informacije prikazane v enem obvestilu na zaslonu. Tako bi se izognili zasičenosti z informacijami in hkrati zagotovili učinkovitost informacij.

79. Navedene smernice pojasnjujejo tudi, da se lahko upravljavci odločijo za uporabo dodatnih orodij za zagotavljanje informacij posamezniku, na katerega se nanašajo osebni podatki, kot so nadzorne plošče za zasebnost. Nadzorna plošča za zasebnost je enotna točka, na kateri si lahko posamezniki, na katere se nanašajo osebni podatki, ogledajo „informacije o zasebnosti“ in upravljajo svoje preference glede zasebnosti, pri čemer zadevnemu upravljavcu dovolijo ali preprečijo določene uporabe svojih podatkov[39]. Nadzorna plošča za zasebnost lahko zagotovi pregled tretjih ponudnikov storitev, ki so od posameznikov, na katere se nanašajo osebni podatki, pridobili izrecno

[38] Člen 14(3)(b) Splošne uredbe o varstvu podatkov.

[39] V skladu s Smernicami Delovne skupine iz člena 29 o preglednosti na podlagi Uredbe(EU) 2016/679, ki jih je potrdil Evropski odbor za varstvo podatkov, so nadzorne plošče za zasebnost koristne zlasti, ko posamezniki, na katere se nanašajo osebni podatki, uporabljajo isto storitev na različnih napravah, saj s tem pridobijo dostop do svojih osebnih podatkov in nadzor nad njimi ne glede na to, kako storitev uporabljajo. To, da lahko posamezniki, na katere se nanašajo osebni podatki, ročno prilagodijo svoje nastavitve zasebnosti prek nadzorne plošče za zasebnost, lahko tudi olajša prilagoditev izjave o varstvu osebnih podatkov z upoštevanjem le tistih vrst obdelave, ki se izvajajo za zadevnega posameznika, na katerega se nanašajo osebni podatki.

privolitev, zagotavlja pa lahko tudi relevantne informacije o naravi in količini osebnih podatkov, do katerih so dostopali tretji ponudniki storitev. Načeloma lahko ponudnik plačilnih storitev, ki vodi račun, uporabniku v okviru pregleda ponudi možnost preklica konkretnega izrecnega soglasja iz direktive PSD2[40], kar bi pomenilo zavrnitev dostopa do njegovih plačilnih računov za enega ali več tretjih ponudnikov storitev. Uporabnik bi lahko od ponudnika plačilnih storitev, ki vodi račune, zahteval tudi, naj enemu ali več določenim tretjim ponudnikom storitev zavrne dostop do njegovega(-ih) plačilnega(-ih) računa(-ov)[41], saj ima uporabnik pravico, da storitev zagotavljanja informacij o računih koristi ali pa ne. Če se nadzorne plošče za zasebnost uporabljajo za dajanje ali preklic izrecnega soglasja, bi morale biti zasnovane in se uporabljati zakonito ter zlasti preprečevati ustvarjanje ovir za pravico tretjih ponudnikov storitev, da opravljajo storitve v skladu z direktivo PSD2. Glede tega in v skladu z veljavnimi določbami iz direktive PSD2 ima tretji ponudnik storitev možnost, da izrecno soglasje od uporabnika vnovič pridobi, potem ko je bilo to soglasje preklicano.

80. Načelo odgovornosti od upravljavca zahteva, naj določi ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da se obdelava izvaja v skladu s Splošno uredbo o varstvu podatkov, zlasti z glavnimi načeli varstva podatkov iz člena 5(1). Taki ukrepi bi morali upoštevati naravo, obseg, okoliščine in namene obdelave ter tveganja za pravice in svoboščine posameznikov, po potrebi pa jih je treba pregledati in dopolniti[42].

6.5 Oblikovanje profilov

81. Obdelava osebnih podatkov, ki jo izvajajo ponudniki plačilnih storitev, lahko vključuje „oblikovanje profilov“ iz člena 4(4) Splošne uredbe o varstvu podatkov. Ponudniki storitev zagotavljanja informacij o računih bi lahko na primer z avtomatizirano obdelavo osebnih podatkov ocenili nekatere osebne vidike glede posameznika. Odvisno od podrobnosti storitve bi se lahko ocenil finančni položaj posameznika, na katerega se nanašajo osebni podatki. Storitve zagotavljanja informacij, ki se zagotovijo na zahtevo uporabnikov, lahko vključujejo obsežno oceno osebnih podatkov plačilnega računa.

82. Upravljavec mora prav tako biti odkrit do posameznika, na katerega se nanašajo osebni podatki, v zvezi z obstojem avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov. V takih primerih mora upravljavec zagotoviti smiselne informacije o razlogih zanj kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki (člena 13(2)(f) in 14(2)(g) ter uvodna izjava 60)[43]. Podobno ima posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 15 Splošne uredbe o varstvu podatkov pravico, da od upravljavca zahteva in pridobi informacije o obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, o razlogih zanj in posledicah za posameznika, na katerega se nanašajo osebni podatki, ter v določenih okoliščinah pravico do ugovora oblikovanju profilov, ne glede na to, ali se izvaja zgolj avtomatizirano sprejemanje posameznih odločitev, ki temelji na oblikovanju profilov[44].

83. Poleg tega je v tem kontekstu pomembna tudi pravica posameznika, na katerega se nanašajo osebni podatki, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva,

[40] Glej na primer „izrecno soglasje“ v členu 67(2)(a) direktive PSD2.
[41] Glej tudi mnenje EBA/OP/2020/10, odstavek 45.
[42] Člen 5(2) in člen 24 Splošne uredbe o varstvu podatkov.
[43] Smernice o preglednosti na podlagi Uredbe (EU) 2016/679, WP 260 rev. 01, ki jih je potrdil Evropski odbor za varstvo podatkov.
[44] Smernice Delovne skupine iz člena 29 o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, WP 251 rev. 01.

kot je določeno v členu 22 Splošne uredbe o varstvu podatkov. Ta norma v določenih okoliščinah vključuje tudi potrebo, da upravljavci podatkov izvedejo ustrezne ukrepe za zaščito pravic posameznika, na katerega se nanašajo osebni podatki, kot so konkretna seznanitev posameznika, na katerega se nanašajo osebni podatki, pravica do človekovega posredovanja pri sprejemanju odločitev, pravica do izražanja lastnega stališča in pravica do izpodbijanja odločitve. Kot je navedeno tudi v uvodni izjavi 71 Splošne uredbe o varstvu podatkov, to med drugim pomeni, da imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da zanje ne velja odločitev, kot je na primer avtomatska zavrnitev spletne prošnje za posojilo brez človekovega posredovanja[45].

84. Avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov, ki vključuje posebne vrste osebnih podatkov, je dovoljeno le, če sta kumulativno izpolnjena pogoja iz člena 22(4) Splošne uredbe o varstvu podatkov:

   – obstaja veljavna izjema iz člena 22(2)

   – in uporabljata se odstavek (a) ali (g) člena 9(2) Splošne uredbe o varstvu podatkov. V obeh primerih upravljavec vzpostavi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki[46].

85. Upoštevati bi bilo treba tudi zahteve za nadaljnjo obdelavo, kot so navedene v teh smernicah. Pojasnila in navodila v zvezi z avtomatiziranim sprejemanjem posameznih odločitev in oblikovanjem profilov, navedena v Smernicah Delovne skupine iz člena 29 o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, kot jih je potrdil Evropski odbor za varstvo podatkov, so v kontekstu plačilnih storitev v celoti relevantna in bi jih bilo zato treba ustrezno upoštevati.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

[45] Uvodna izjava 71 Splošne uredbe o varstvu podatkov.
[46] Smernice Delovne skupine iz člena 29 o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, WP 251 rev. 01, stran 24.