Smjernice

Smjernice 3/2022 o obmanjujućim obrascima dizajna na sučeljima platformi društvenih medija: kako ih prepoznati i izbjeći

Verzija 2.0

Donesene 14. veljače 2023.

Pregled verzija

Verzija 2.0	14. veljače 2023.	Donošenje Smjernica nakon javnog savjetovanja
Verzija 1.0	14. ožujka 2022.	Donošenje Smjernica za javno savjetovanje

SAŽETAK

U ovim se Smjernicama pružateljima usluga društvenih medija kao voditeljima obrade podataka na društvenim medijima, dizajnerima i korisnicima platformi društvenih medija daju praktične preporuke o tome kako procijeniti i izbjeći takozvane „obmanjujuće obrasce dizajna" na sučeljima društvenih medija koja krše zahtjeve Opće uredbe o zaštiti podataka (OUZP). U tu svrhu Europski odbor za zaštitu podataka (EDPB) preporučuje da voditelji obrade okupe interdisciplinarne timove koji će među ostalim uključivati dizajnere, službenike za zaštitu podataka i donositelje odluka. Važno je napomenuti da popisi obmanjujućih obrazaca dizajna i primjera dobre prakse, kao i scenarija uporabe, nisu potpuni. Pružatelji usluga društvenih medija i dalje su odgovorni za usklađivanje svojih platformi s OUZP-om.

Obmanjujući obrasci dizajna na sučeljima platformi društvenih medija

U kontekstu ovih Smjernica „obmanjujućim obrascima dizajna" smatraju se sučelja i korisnička putovanja na platformama društvenih medija kojima se pokušava utjecati na korisnike kako bi donijeli nenamjerne, neželjene i potencijalno štetne odluke o obradi svojih osobnih podataka, koje su često protivne njihovu najboljem interesu i pogoduju interesima platformi društvenih medija. Obmanjujući obrasci dizajna utječu na ponašanje korisnika i mogu ograničiti njihovu sposobnost zaštite osobnih podataka i svjesnog odlučivanja. Tijela za zaštitu podataka dužna su sankcionirati primjenu obmanjujućih obrazaca dizajna ako oni krše zahtjeve OUZP-a. Obmanjujući obrasci dizajna obuhvaćeni ovim Smjernicama mogu se podijeliti u sljedeće kategorije:

- ***Preopterećenost*** znači da se korisnici izlažu velikoj količini zahtjeva, informacija, opcija ili mogućnosti kako bi ih se potaknulo da podijele više podataka ili nenamjerno dopuste obradu osobnih podataka protivno očekivanjima ispitanika.
  Ovoj kategoriji pripadaju sljedeće tri vrste obmanjujućih obrazaca dizajna: ***kontinuirano prikazivanje upita***, ***labirint pravila privatnosti*** i ***previše opcija***.

- ***Preskakanje*** znači dizajniranje sučelja ili korisničkog putovanja tako da korisnici zaborave ili ne razmišljaju o svim ili nekim aspektima zaštite podataka.
  Ovoj kategoriji pripadaju sljedeće dvije vrste obmanjujućih obrazaca dizajna: ***obmanjujući komfor*** i ***odvraćanje pozornosti***.

- ***Stimuliranje*** utječe na izbor korisnika pobuđivanjem emocija ili vizualnim poticajima.
  Ovoj kategoriji pripadaju sljedeće dvije vrste obmanjujućih obrazaca dizajna: ***upravljanje emocijama*** i ***skrivanje na vidljivom mjestu***.

- ***Ometanje*** znači sprečavanje ili blokiranje nastojanja korisnika da se informiraju ili upravljaju svojim podacima time što im se to otežava ili onemogućuje.
  Ovoj kategoriji pripadaju sljedeće tri vrste obmanjujućih obrazaca dizajna: ***slijepa ulica***, ***dulje trajanje od nužnog*** i ***zavaravajuća radnja***.

- ***Nestalnost*** znači da je dizajn sučelja nedosljedan i nejasan, što korisniku otežava navigaciju alatima za nadzor zaštite podataka i razumijevanje svrhe obrade.

Ovoj kategoriji pripadaju sljedeće četiri vrste obmanjujućih obrazaca dizajna: ***nedostatak hijerarhije, dekontekstualizacija, nedosljedno sučelje*** i ***jezični diskontinuitet***.

- ***Držanje u neznanju*** znači da je sučelje dizajnirano tako da se prikriju informacije ili alati za nadzor zaštite podataka ili da korisnici nisu sigurni kako se njihovi podaci obrađuju i kako ih mogu nadzirati u smislu ostvarivanja svojih prava.
  Ovoj kategoriji pripadaju sljedeće dvije vrste obmanjujućih obrazaca dizajna: ***proturječne informacije*** i ***dvosmisleni tekst ili informacije***.

Relevantne odredbe OUZP-a za procjenu obmanjujućih obrazaca dizajna

Načela primjenjiva na usklađenost korisničkih sučelja internetskih aplikacija u sektoru društvenih medija s pravilima o zaštiti podataka utvrđena su u članku 5. OUZP-a. Načelo poštene obrade utvrđeno u članku 5. stavku 1. točki (a) OUZP-a polazište je za procjenu je li određeni obrazac dizajna obmanjujući. Za tu su procjenu važna i načela transparentnosti, smanjenja količine podataka i pouzdanosti u skladu s člankom 5. stavkom 1. točkama (a), (c) i stavkom 2. OUZP-a te, u određenim slučajevima, ograničavanja svrhe u skladu s člankom 5. stavkom 1. točkom (b) OUZP-a. U ostalim slučajevima pravna procjena temelji se i na uvjetima privole iz članka 4. stavka 11. i članka 7. OUZP-a ili drugim posebnim obvezama, kao što su one iz članka 12. OUZP-a. Očito je da je u kontekstu prava ispitanika potrebno uzeti u obzir i treće poglavlje OUZP-a. Naposljetku, zahtjevi tehničke i integrirane zaštite podataka iz članka 25. OUZP-a imaju važnu ulogu jer bi pružatelji usluga društvenih medija njihovom primjenom prije uvođenja određenog dizajna sučelja posve izbjegli obmanjujuće obrasce dizajna.

Primjeri obmanjujućih obrazaca dizajna u scenarijima uporabe tijekom životnog ciklusa računa na društvenim medijima

Odredbe OUZP-a primjenjuju se na cijeli tijek obrade osobnih podataka u okviru rada platformi društvenih medija, tj. na cijeli životni ciklus korisničkog računa. EDPB navodi konkretne primjere obmanjujućih obrazaca dizajna za sljedeće scenarije uporabe u životnom ciklusu: izrada računa, tj. postupak registracije; scenariji uporabe informacija koji se odnose na obavijest o zaštiti privatnosti, zajedničko vođenje obrade i obavješćivanje o povredi podataka; upravljanje privolama i zaštitom podataka; ostvarivanje prava ispitanika tijekom korištenja društvenih medija i, naposljetku, zatvaranje računa na društvenim medijima. Povezanost s odredbama OUZP-a objašnjena je na dva načina: prvo, za svaki se scenarij uporabe detaljnije objašnjava koja je od navedenih odredbi OUZP-a posebno relevantna za njega. Drugo, u odlomcima koji se odnose na primjere obmanjujućih obrazaca dizajna objašnjava se kako se njima krši OUZP.

Preporuke dobre prakse

Osim primjera obmanjujućih obrazaca dizajna u Smjernicama se na kraju svakog scenarija uporabe, kao i u Prilogu II., navode primjeri dobre prakse. Oni sadržavaju posebne preporuke za dizajniranje korisničkih sučelja koje olakšavaju učinkovitu provedbu OUZP-a.

Kontrolni popis kategorija obmanjujućih obrazaca dizajna

Kontrolni popis kategorija obmanjujućih obrazaca dizajna nalazi se u Prilogu I. ovim Smjernicama. Sadržava pregled navedenih kategorija i vrsta obmanjujućih obrazaca dizajna, kao i popis primjera za svaki obrazac koji se spominju u scenarijima uporabe. Nekim čitateljima taj kontrolni popis može poslužiti kao korisna početna točka za proučavanje ovih Smjernica.

Sadržaj

1. Područje primjene 8
2. Primjenjiva načela – što treba imati na umu? 11
2.1. Pouzdanost 12
2.2. Transparentnost 12
2.3. Tehnička i integrirana zaštita podataka 13
3. Životni ciklus računa na društvenim medijima: primjena načela u praksi 15
3.1. Otvaranje računa na društvenim medijima 15
Scenarij uporabe 1: registracija računa 15
3.2. Informiranje na društvenim medijima 26
Scenarij uporabe 2a: slojevita obavijest o zaštiti privatnosti 26
Scenarij uporabe 2b: informiranje ispitanika o zajedničkom vođenju obrade, članak 26. stavak 2. OUZP-a 32
Scenarij uporabe 2c: obavješćivanje ispitanika o povredi osobnih podataka 33
3.3. Zaštita na društvenim medijima 36
Scenarij uporabe 3a: upravljanje privolom za vrijeme korištenja platforme društvenih medija 36
Scenarij uporabe 3b: upravljanje postavkama zaštite podataka 43
3.4. Prava na društvenim medijima prava ispitanika 50
Scenarij uporabe 4: kako osigurati odgovarajuće funkcije za ostvarivanje prava ispitanika 50
3.5. Vrijeme je za oproštaj: zatvaranje računa na društvenim medijima 57
Scenarij uporabe 5: pauziranje računa / brisanje svih osobnih podataka 57
4. Prilog I.: Popis kategorija i vrsta obmanjujućih obrazaca dizajna 65
4.1. Preopterećenost 65
4.1.1. Kontinuirano prikazivanje upita 65
4.1.2. Labirint pravila privatnosti 65
4.1.3. Previše opcija 66
4.2. Preskakanje 66
4.2.1. Obmanjujući komfor 66
4.2.2. Odvraćanje pozornosti 67
4.3. Stimuliranje 67
4.3.1. Upravljanje emocijama 67
4.3.2. Skrivanje na vidljivom mjestu 67
4.4. Ometanje 68
4.4.1. Slijepa ulica 68
4.4.2. Dulje trajanje od nužnog 68

4.4.3. Zavaravajuća radnja 69
4.5. Nestalnost 69
4.5.1. Nedostatak hijerarhije 69
4.5.2. Dekontekstualizacija 69
4.5.3. Nedosljedno sučelje 69
4.5.4. Jezični diskontinuitet 70
4.6. Držanje u neznanju 70
4.6.1. Proturječne informacije 70
4.6.2. Dvosmisleni tekst ili informacije 71
5. Prilog II.: Primjeri dobre prakse 73

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 „OUZP"),

uzimajući u obzir Sporazum o EGP-u, a 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,

DONIO JE SLJEDEĆE SMJERNICE:

1. PODRUČJE PRIMJENE

1. Cilj je ovih Smjernica pružiti preporuke i upute za dizajn sučelja platformi društvenih medija. Za potrebe ovih Smjernica društveni mediji su internetske platforme koje omogućuju razvoj mreža i zajednica korisnika koji razmjenjuju informacije i sadržaje[2]. Smjernice se mogu slijediti u fazi osmišljavanja korisničkog sučelja kako bi se od početka izbjegla primjena obmanjujućih obrazaca dizajna[3] ili u okviru postojeće usluge kako bi se ocijenila usklađenost njezina sučelja. Namijenjene su pružateljima usluga društvenih medija kao voditeljima obrade podataka na društvenim medijima, koji su odgovorni za dizajn i rad platformi društvenih medija. U tom je smislu cilj Smjernica podsjetiti na obveze koje proizlaze iz OUZP-a, ponajprije na načela zakonitosti, poštenosti, transparentnosti, ograničavanja svrhe i smanjenja količine podataka u dizajnu korisničkih sučelja i prikazu sadržaja njihovih internetskih usluga i aplikacija. Navedena načela moraju se temeljito provesti i s tehničkog stajališta predstavljaju zahtjeve za dizajn softvera i usluga, uključujući korisnička sučelja. Detaljno se razmatra primjena zahtjeva OUZP-a na korisnička sučelja i prikaz sadržaja te se pojašnjava što bi trebalo smatrati „obmanjujućim obrascem dizajna", odnosno načinom osmišljavanja i prikaza sadržaja kojim se ti zahtjevi u znatnoj mjeri krše, iako se ostavlja dojam da su formalno ispunjeni. U ovim se Smjernicama korisnici mogu i informirati o pravima i rizicima koji mogu proizaći iz razmjene prevelike količine podataka ili nekontroliranog dijeljenja njihovih podataka. Osim toga, cilj je ovih Smjernica educirati korisnike kako bi prepoznali „obmanjujuće obrasce dizajna" (kako su definirani u nastavku) i kako pri susretu s njima svjesno zaštititi svoju privatnost. Analiza je obuhvaćala životni ciklus računa na društvenim medijima na temelju pet scenarija uporabe: „otvaranje računa na društvenim medijima" (scenarij uporabe 1), „informiranje na društvenim medijima" (scenarij uporabe 2), „zaštita na društvenim medijima" (scenarij uporabe 3), „ostvarivanje prava na društvenim medijima: prava ispitanika" (scenarij uporabe 4) i „vrijeme je za oproštaj: zatvaranje računa na društvenim medijima" (scenarij uporabe 5).

[1] Upućivanja na „države članice" u ovom dokumentu treba tumačiti kao upućivanja na „države članice EGP-a".
[2] Definicija je istovjetna onoj u Smjernicama EDPB-a 8/2020 o ciljanju korisnika društvenih medija, točki 1., vidjeti bilješku 1 za podrobniji opis; dostupno na https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hr_0.pdf.
[3] U verziji 2.0 ovih Smjernica EDPB koristi uključiviji opisni pojam „obmanjujući obrazac dizajna" umjesto pojma „tamni obrazac".

2. U ovim Smjernicama pojam „korisničko sučelje" odnosi se na sredstvo za interakciju s platformama društvenih medija. Tema su ovog dokumenta grafička korisnička sučelja (npr. za računala i pametne telefone), ali određena opažanja mogu se primijeniti i na sučelja s glasovnim upravljanjem (npr. za pametne zvučnike) ili sučelja kojima se upravlja pokretom (npr. za virtualnu stvarnost). Pojam „korisničko putovanje" odnosi se na niz radnji ili koraka koje korisnici trebaju izvršiti kako bi postigli svoj cilj, koji na društvenim mrežama može biti pregledavanje objava, dijeljenje objave, prilagodba preferencija itd. Pojam „korisničko iskustvo" odnosi se na ukupno iskustvo korisnika na platformi društvenih medija, što uključuje percipiranu korisnost, jednostavnost uporabe i učinkovitost interakcije s platformom. Dizajn korisničkog sučelja i korisničkog iskustva kontinuirano su se razvijali u proteklom desetljeću. U posljednje vrijeme u prvom je planu stvaranje sveprisutnih, prilagođenih i takozvanih neometanih korisničkih interakcija i iskustava: savršeno sučelje trebalo bi biti iznimno personalizirano, jednostavno za korištenje i multimodalno[4]. Iako bi zahvaljujući tim trendovima korištenje digitalnih usluga moglo postati jednostavnije, oni bi se ponajprije mogli iskoristiti za poticanje korisnika na ponašanje protivno načelima OUZP-a[5]. To je posebno važno u kontekstu „ekonomije pozornosti", u kojoj se pozornost korisnika smatra robom. U tim se slučajevima mogu prekoračiti zakonski dopuštene granice OUZP-a, a dizajn sučelja i dizajn korisničkog iskustva koji dovode do toga opisani su u nastavku kao „obmanjujući obrasci dizajna".

3. U kontekstu ovih Smjernica „obmanjujućim obrascima dizajna" smatraju se sučelja i korisnička putovanja na platformama društvenih medija kojima se nastoji utjecati na korisnike kako bi donijeli nenamjerne odnosno neželjene i/ili potencijalno štetne odluke o obradi svojih osobnih podataka, koje su često protivne njihovu najboljem interesu i pogoduju interesima platformi društvenih medija. Cilj je obmanjujućih obrazaca dizajna utjecati na ponašanje korisnika, uglavnom na temelju kognitivne pristranosti. Oni mogu ograničiti sposobnost korisnika da „zaštite svoje osobne podatke i donose svjesne odluke"[6], na primjer tako da im onemoguće „davanje informirane i dobrovoljne privole"[7]. To se može zloupotrijebiti u više aspekata dizajna, kao što su odabir boja sučelja i raspored sadržaja. S druge strane, poticaji i dizajn prilagođen korisnicima mogu pridonijeti provedbi propisa o zaštiti podataka.

4. Obmanjujući obrasci dizajna ne dovode nužno samo do kršenja propisa o zaštiti podataka. Iz tih obrazaca može, na primjer, proizaći i povreda propisa o zaštiti potrošača. Granice između kršenja u nadležnosti tijela za zaštitu podataka i onih u nadležnosti nacionalnih tijela za zaštitu potrošača, tijela za tržišno natjecanje ili drugih tijela mogu se preklapati[8]. U skladu s OUZP-om tijela za zaštitu podataka odgovorna su za sankcioniranje primjene obmanjujućih obrazaca dizajna ako se njima zaista krše standardi zaštite podataka, a time i OUZP. Povrede zahtjeva OUZP-a potrebno je procijeniti na

[4] Za više pojedinosti vidjeti CNIL, *IP Report No. 6: Shaping Choices in the Digital World*, 2019. str. 9. https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[5] CNIL, *Shaping Choices in the Digital World*, 2019. str. 10.

[6] CNIL, *Shaping Choices in the Digital World*, 2019. str. 27.

[7] Vidjeti Norveško vijeće potrošača, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, str. 10. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, ali i CNIL, *Shaping Choices in the Digital World*, str. 30., 31.

[8] U tom se smislu u članku 25. stavku 2. Uredbe (EU) 2022/2065 od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) pojašnjava da se zabrana obmanjujućeg ili manipulativnog dizajna internetskih sučelja iz njezina članka 25. stavka 1. ne primjenjuje na prakse obuhvaćene Direktivom 2005/29/EZ (Direktiva o nepoštenoj poslovnoj praksi poslovnog subjekta u odnosu prema potrošaču) ili OUZP-om. Osim toga, u Obavijesti Komisije EU-a (2021/C 526/01) navedene su smjernice za tumačenje i primjenu Direktive o nepoštenoj poslovnoj praksi, uključujući „tamne uzorke" u točki 4.2.7.

pojedinačnoj osnovi. Ove Smjernice odnose se samo na obmanjujuće obrasce dizajna koji bi mogli biti obuhvaćeni tom regulatornom ovlašću. Iz tog razloga, osim primjera obmanjujućih obrazaca dizajna, u Smjernicama su navedeni i primjeri dobre prakse za dizajniranje korisničkih sučelja koja će olakšati djelotvornu provedbu OUZP-a. Ti primjeri dobre prakse mogu biti prvi korak prema standardiziranom postupku kojim će korisnici učinkovito nadzirati svoje podatke i ostvarivati svoja prava.

5. Obmanjujući obrasci dizajna[9] koji se obrađuju u ovim Smjernicama proizlaze iz interdisciplinarne analize postojećih sučelja i mogu se podijeliti u sljedeće kategorije:

Preopterećenost: korisnici se izlažu velikoj količini zahtjeva, informacija, opcija ili mogućnosti kako bi ih se potaknulo da podijele više podataka ili nenamjerno dopuste obradu osobnih podataka protivno očekivanjima ispitanika.

Preskakanje: dizajniranje sučelja ili korisničkog putovanja tako da korisnici zaborave ili ne razmišljaju o svim ili nekim aspektima zaštite podataka.

Stimuliranje: utjecanje na izbor korisnika pobuđivanjem emocija ili vizualnim poticajima.

Ometanje: ometanje ili blokiranje korisnika u njihovim nastojanjima da se informiraju ili da upravljaju svojim podacima time što im se to otežava ili onemogućuje.

Nestalnost: dizajn sučelja nedosljedan je i nejasan, što korisnicima otežava navigaciju alatima za nadzor zaštite podataka i razumijevanje svrhe obrade.

Držanje u neznanju: sučelje je dizajnirano tako da se prikriju informacije ili alati za nadzor zaštite podataka ili da korisnici nisu sigurni kako se njihovi podaci obrađuju i kako kontrolu nad njima mogu imati u smislu ostvarivanja svojih prava.

6. Osim ponovnog razvrstavanja obmanjujućih obrazaca dizajna u kategorije u skladu s njihovim učincima na ponašanje korisnika, oni se mogu podijeliti i na obrasce koji se temelje na sadržaju i one koji se temelje na sučelju kako bi se konkretnije obuhvatili aspekti korisničkog sučelja ili korisničkog putovanja. Obrasci koji se temelje na sadržaju odnose se na stvarni sadržaj, a time i na tekst i kontekst rečenica i elemenata informacija. Međutim, određeni elementi izravno utječu i na percepciju tih čimbenika. Ti obrasci koji se temelje na sučelju povezani su s načinima prikazivanja sadržaja, navigacije ili interakcije s njim.

7. Važno je imati na umu da su obmanjujući obrasci dizajna problematični i zbog mogućeg utjecaja na djecu[10] koja se registriraju na platformi društvenih medija, ali i na druge ranjive skupine, kao što su starije osobe, osoba s oštećenjem vida ili osobe koje nisu digitalno pismene kao ostali. Ranjive skupine kao što su stariji korisnici često nisu samo manje sposobne prepoznati manipulativni dizajn, već su i manje svjesne toga da se utječe na njihovo digitalno ponašanje. U OUZP-u propisane su dodatne zaštitne mjere kad se obrada odnosi na osobne podatke djece jer ona mogu biti manje svjesna predmetnih rizika i posljedica te svojih prava povezanih s obradom[11]. U uvodnoj izjavi 58. izričito se navodi da bi se, u slučaju da je obrada usmjerena prema djetetu, svaka informacija trebala pružati na jasnom i jednostavnom jeziku koji djeca lako mogu razumjeti. Osim toga, u OUZP-u je obrada podataka pojedinaca, posebno djece, izričito uvrštena među situacije u kojima rizik za prava i obveze pojedinaca,

[9] Kategorije obmanjujućih obrazaca dizajna i vrste obmanjujućih obrazaca dizajna unutar tih kategorija u tekstu Smjernica bit će navedene ***podebljanim slovima i u kurzivu***. Detaljan pregled nalazi se u Prilogu.
[10] Vidjeti i uvodnu izjavu 81. četvrtu rečenicu Uredbe (EU) 2022/2065 (Akt o digitalnim uslugama).
[11] Uvodna izjava 38. OUZP-a.

različitih vjerojatnosti i ozbiljnosti, može proizaći iz obrade podataka koja bi mogla prouzročiti fizičku, materijalnu ili nematerijalnu štetu[12].

8. Uzimajući u obzir prethodno navedeno, treba biti jasno da obmanjujući obrasci dizajna nisu prisutni samo na platformama društvenih medija. Za vrijeme javnog savjetovanja o ovim Smjernicama o tom su pitanju iznesena podijeljena mišljenja. Sučelja su prisutna u mnogim drugim slučajevima kad korisnici stupaju u interakciju s proizvodima i uslugama koji se temelje na obradi podataka ili su s njom povezani. To može uključivati internetske stranice i obavijesti o kolačićima[13], internetske trgovine, videoigre, mobilne aplikacije ili mikroplaćanja. Iako obmanjujući obrasci dizajna opisani u nastavku možda nisu prisutni u potpuno istom obliku, njihove inačice i dalje mogu kršiti prava ispitanika ili potrošača. Međutim, ove Smjernice odnose se isključivo na obmanjujuće obrasce dizajna na platformama društvenih medija jer one sve više utječu na svakodnevni život ljudi i nacija, što se jasno vidi iz prethodnih dokumenata EDPB-a[14].

2. PRIMJENJIVA NAČELA – ŠTO TREBA IMATI NA UMU?

9. Načela primjenjiva na usklađenost korisničkih sučelja internetskih aplikacija u sektoru društvenih medija s pravilima o zaštiti podataka utvrđena su u članku 5. OUZP-a. Načelo poštene obrade utvrđeno u članku 5. stavku 1. točki (a) OUZP-a polazište je za procjenu prisutnosti obmanjujućih obrazaca dizajna. Kao što je EDPB već naveo, poštenost je sveobuhvatno načelo kojim se zahtijeva da se osobni podaci ne obrađuju na način koji je štetan, diskriminirajući, neočekivan ili zavaravajući za ispitanika[15]. Ako sučelje ne sadržava dovoljno informacija za korisnike ili su one zavaravajuće te ima obilježja obmanjujućih obrazaca dizajna, može se klasificirati kao nepoštena obrada. Načelo poštenosti ima krovnu funkciju i nijedan obmanjujući obrazac dizajna ne bi bio u skladu s njim neovisno o tome je li usklađen s drugim načelima zaštite podataka.

10. Osim te temeljne odredbe o poštenosti obrade, za okvir dizajna relevantna su i načela pouzdanosti i transparentnosti te obveza tehničke zaštite podataka navedena u članku 25. OUZP-a, a obmanjujući obrasci dizajna mogli bi kršiti te odredbe. Međutim, pravna procjena obmanjujućih obrazaca dizajna može se temeljiti i na elementima općih definicija kao što je definicija privole iz članka 4. točke 11. OUZP-a ili drugim posebnim obvezama kao što su one iz članka 12. OUZP-a. U skladu s člankom 12. stavkom 1. prvom rečenicom OUZP-a voditelji obrade dužni su poduzeti odgovarajuće mjere kako bi se sve komunikacije povezane s pravima ispitanika, kao i sve informacije, pružale u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika

[12] Uvodna izjava 75. OUZP-a; vidjeti i Smjernice EDPB-a 8/2020 o ciljanju korisnika društvenih medija, točku 16. https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hr_0.pdf.

[13] Potaknuti pritužbama organizacije NOYB članovi radne skupine EDPB-a razmijenili su mišljenja o nizu elemenata dizajna u obavijestima o kolačićima. Zajednički nazivnik koji su nadzorna tijela dogovorila u svojem tumačenju primjenjivog višeslojnog pravnog okvira sažet je u „Izvješću o radu radne skupine za obavijesti o kolačićima" od 17. siječnja 2023., dostupnom na https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

[14] Smjernice EDPB-a 8/2020 o ciljanju korisnika društvenih medija, Izjava 2/2019 o korištenju osobnih podataka tijekom političkih kampanja https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_en.

[15] Smjernice EDPB-a 4/2019 o članku 25., Tehnička i integrirana zaštita podataka, verzija 2.0, donesene 20. listopada 2020., str. 16.; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_hr.

Međutim, kao što je vidljivo iz uvodne izjave 39. treće rečenice o načelu transparentnosti, taj zahtjev nije ograničen na obavijesti o zaštiti podataka[16] ili prava ispitanika[17], nego se primjenjuje na sve informacije i komunikaciju o obradi osobnih podataka. U petoj rečenici te uvodne izjave pojašnjava se i da bi ispitanici trebali biti upoznati s rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom osobnih podataka i načinom ostvarenja svojih prava u vezi s obradom.

11. Za dizajn korisničkih sučelja internetskih aplikacija važno je uzeti u obzir i načelo ograničavanja svrhe iz članka 5. stavka 1. točke (b) OUZP-a, kao i načelo smanjenja količine podataka iz članka 5. stavka 1. točke (c) OUZP-a. U svakom slučaju, kako bi se postigla usklađenost u području zaštite podataka, voditeljima obrade savjetuje se da dobro provjere usklađenost sa svim načelima zaštite podataka iz OUZP-a.

2.1. Pouzdanost

12. Svako korisničko sučelje mora se dizajnirati u skladu s načelom pouzdanosti.

13. U članku 5. stavku 2. OUZP-a navodi se da je voditelj obrade odgovoran za usklađenost s načelima OUZP-a opisanima u njegovu članku 5. stavku 1. te je mora biti u mogućnosti dokazati. Dakle, to je načelo usko povezano s navedenim relevantnim načelima. Pouzdanost se može postići elementima koji dokazuju usklađenost pružatelja usluga društvenih medija s OUZP-om. Korisničko sučelje i korisničko putovanje mogu poslužiti kao alat za dokumentiranje koji dokazuje da su korisnici pri obavljanju radnji na platformi društvenih medija pročitali i uzeli u obzir informacije o zaštiti podataka, dali dobrovoljnu privolu, lako ostvarili svoja prava itd. Usklađenost se može dokazati i na temelju rezultata i analize kvalitativnih i kvantitativnih metoda istraživanja korisnika, kao što su A/B testiranje, praćenje kretanja očiju ili intervjui s korisnicima. Važno je napomenuti da takve metode istraživanja često uključuju i obradu osobnih podataka, koja zato mora biti u skladu s OUZP-om. Na primjer, ako korisnici moraju označiti polje ili kliknuti na jednu od nekoliko opcija zaštite podataka, snimke zaslona sučelja mogu prikazati putanju korisnika kroz informacije o zaštiti podataka i objasniti kako korisnici donose svjesnu odluku. Rezultati istraživanja korisnika provedenog na tom sučelju pružili bi dodatne elemente koji pokazuju zašto je to sučelje optimalno za postizanje cilja informiranja.

14. U području korisničkih sučelja takvi se elementi za dokumentiranje koriste pri objavi određenih ugovora i, prije svega, pri pribavljanju dokaza, na primjer o davanju privole ili potvrde o čitanju.

2.2. Transparentnost

15. Načelo transparentnosti iz članka 5. stavka 1. točke (a) OUZP-a uvelike se preklapa s područjem opće pouzdanosti. Iako voditelji obrade moraju štititi određene osjetljive poslovne informacije koje se dijele s trećim stranama, odobravanje pristupa dokumentaciji o obradi ili njezino evidentiranje moglo bi pridonijeti postizanju pouzdanosti: na primjer, za tekst koji voditelj obrade mora staviti na raspolaganje u skladu s načelom transparentnosti može se dobiti potvrda o čitanju. Tako se ujedno može zajamčiti transparentnost prema ispitanicima.

16. Sva načela zaštite podataka iz članka 5. OUZP-a dodatno su razrađena u toj uredbi. Člankom 5. stavkom 1. točkom (a) OUZP-a propisuje se da se osobni podaci obrađuju transparentno s obzirom na ispitanika. U Smjernicama o transparentnosti navedeni su elementi transparentnosti kako su utvrđeni u članku 12. OUZP-a, tj. potreba za pružanjem informacija u „sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika"[18]. Te smjernice sadržavaju i upute o

[16] Obrađeno u dijelu 3.2. – scenarij uporabe 2a ovih Smjernica.
[17] Obrađeno u scenarijima uporabe 4 i 5, tj. dijelovima 3.4. i 3.5. ovih Smjernica.
[18] Smjernice Radne skupine iz članka 29. o transparentnosti na temelju Uredbe 2016/679, koje je potvrdio EDPB https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

tome kako pružatelji usluga društvenih medija mogu ispuniti obveze informiranja u skladu s člancima 13. i 14. OUZP-a.

17. Osim toga, tekst načela zaštite podataka iz članka 5. stavka 1. točke (a) OUZP-a i druge posebne pravne odredbe Uredbe sadržavaju mnogo više pojedinosti o načelu transparentnosti, koje su povezane s određenim pravnim načelima, kao što su posebni zahtjevi za transparentnost radi dobivanja privole iz članka 7. OUZP-a.

2.3. Tehnička i integrirana zaštita podataka

18. U članku 25. stavku 1. OUZP-a navedeno je da voditelji obrade provode odgovarajuće tehničke i organizacijske mjere za provedbu načela zaštite podataka, dok se u članku 25. stavku 2. pojašnjava da se takve mjere provode i kako bi se osiguralo da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. U kontekstu Smjernica 4/2019 o članku 25. Tehnička i integrirana zaštita podataka postoje ključni elementi koje voditelji obrade i izvršitelji obrade moraju uzeti u obzir pri provedbi tehničke zaštite podataka u okviru platforme društvenih medija. Među ostalim, u skladu s načelom poštenosti informacije o obradi podataka i mogućnosti za njihovu obradu trebale bi se iznositi objektivno i neutralno, tako da se izbjegne svaka vrsta obmanjujućeg ili manipulativnog jezika ili dizajna[19]. U tim se smjernicama među ostalim utvrđuju elementi načela za tehničku i integriranu zaštitu podataka, koji postaju još relevantniji s obzirom na obmanjujuće obrasce dizajna[20]:

- Autonomija – ispitanicima bi se trebala dodijeliti najviša moguća razina autonomije kad je riječ o odlučivanju o uporabi njihovih osobnih podataka te opsegu i uvjetima te uporabe ili obrade.
- Interakcija – ispitanici moraju moći komunicirati o svojim pravima u kontekstu obrade osobnih podataka koju provodi voditelj obrade te ostvarivati svoja prava u tom pogledu.
- Očekivanja – obrada bi trebala biti u skladu s očekivanjima ispitanika.
- Odabir potrošača – voditelj obrade ne smije nepošteno „zaključati" svoje korisnike. Ako je riječ o vlasničkoj usluzi obrade osobnih podataka, može nastati učinak zaključavanja u okviru te usluge, što može biti nepošteno ako se time ispitanicima onemogućuje da ostvaruju svoje pravo prenosivosti podataka u skladu s člankom 20. OUZP-a.
- Ravnoteža moći – ravnoteža moći trebala bi biti ključan cilj odnosa između voditelja obrade i ispitanika. Trebalo bi izbjegavati svaki oblik neravnoteže moći. Kad to nije moguće, trebalo bi je prepoznati i poduzeti odgovarajuće protumjere.
- Zabrana obmanjivanja – informacije o obradi podataka i mogućnosti za njihovu obradu trebale bi se iznositi objektivno i neutralno, tako da se izbjegne svaka vrsta obmanjujućeg ili manipulativnog jezika ili dizajna.
- Istinitost – voditelj obrade mora staviti na raspolaganje informacije o tome kako obrađuje osobne podatke. Trebao bi postupati kako je predvidio i ne smije zavaravati ispitanike.

19. Usklađenost s integriranom i tehničkom zaštitom podataka važna je pri procjeni obmanjujućih obrazaca dizajna jer bi omogućila da se oni izbjegnu. Naime, ocjenjivanje usluge i povezanih sučelja

[19] Vidjeti Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka, str. 18, točku 70.
[20] Izvadak iz teksta – za cijeli popis vidjeti Smjernice o članku 25. Tehnička i integrirana zaštita podataka, točku 70.

prema elementima koji obuhvaćaju načela integrirane i tehničke zaštite podataka, kao što su navedena načela, pomoći će da se prije pokretanja usluge prepoznaju njezini aspekti koji bi mogli predstavljati obmanjujući obrazac dizajna. Na primjer, ako se informacije o zaštiti podataka pružaju bez poštovanja načela zabrane obmanjivanja, vjerojatno je riječ o obmanjujućem obrascu dizajna ***skrivanje na vidljivom mjestu*** ili ***upravljanje emocijama***, koji će se dodatno razraditi u scenariju uporabe 1.

3. ŽIVOTNI CIKLUS RAČUNA NA DRUŠTVENIM MEDIJIMA: PRIMJENA NAČELA U PRAKSI

20. OUZP se primjenjuje na cijeli postupak obrade osobnih podataka koji se obavlja automatizirano[21]. Ako se osobni podaci obrađuju u okviru rada platformi društvenih medija, OUZP i njegova načela primjenjuju se na cijeli životni ciklus korisničkog računa.

3.1. Otvaranje računa na društvenim medijima

Scenarij uporabe 1: registracija računa

a. Opis konteksta

21. Kako bi korisnici mogli pristupiti platformi društvenih medija, prvo se moraju registrirati otvaranjem računa. Tijekom postupka registracije od korisnika se traži da navedu svoje osobne podatke, kao što su ime i prezime, e-adresa, a katkad i broj telefona. Korisnici moraju biti obaviješteni o obradi njihovih osobnih podataka i obično se od njih traži da potvrde da su pročitali obavijest o zaštiti privatnosti i da se slažu s uvjetima korištenja platforme društvenih medija. Te informacije moraju biti navedene jasnim i jednostavnim jezikom kako bi ih korisnici mogli lako razumjeti i svjesno na njih pristati.

22. U toj početnoj fazi postupka registracije korisnici bi trebali razumjeti na što točno pristaju, u smislu da bi predmet dogovora između platforme društvenih medija i korisnika trebao biti što jasnije i jednostavnije opisan.

23. Pružatelji usluga društvenih medija stoga moraju učinkovito uzeti u obzir tehničku zaštitu podataka kako bi zaštitili prava i slobode ispitanika[22].

b. Relevantne pravne odredbe

24. Pružatelji usluga društvenih medija pri dizajniranju svojih sučelja moraju pravilno provoditi načela iz članka 5. OUZP-a. Iako je transparentnost prema ispitanicima uvijek neophodna, posebno je važna u fazi izrade računa na platformi društvenih medija. Zbog svojeg položaja voditelja obrade ili izvršitelja obrade platforme društvenih medija trebale bi korisnicima prilikom prijave učinkovito i sažeto pružiti informacije te bi se one trebale jasno razlikovati od ostalih informacija koje nisu povezane sa zaštitom podataka[23]. Dio obveza transparentnosti voditelja obrade odnosi se na informiranje korisnika o njihovim pravima, među kojima je i pravo na povlačenje privole u bilo kojem trenutku ako je privola primjenjiva pravna osnova[24].

i. Privola dana u fazi registracije

25. Kako je navedeno u članku 4. točki 11. i članku 7. OUZP-a, koji su pojašnjeni u uvodnoj izjavi 32., ako je privola odabrana kao pravna osnova za obradu, ona mora biti „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". Da bi se privola smatrala valjanom, svi navedeni uvjeti moraju biti kumulativno ispunjeni.

[21] Vidjeti članak 2. stavak 1. OUZP-a.
[22] Vidjeti Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka.
[23] Vidjeti Smjernice o transparentnosti, točku 8.
[24] Smjernice o transparentnosti, točka 30. i stranica 39.

26. Smjernice EDPB-a 05/2020 o privoli sadržavaju dragocjene upute za pružatelje društvenih medija koji traže privolu korisnika u razne svrhe obrade[25]. Platforme društvenih medija ne smiju zaobilaziti uvjete, na primjer mogućnost ispitanika da slobodno daju privolu, primjenom grafičkog dizajna ili teksta koji ispitanicima onemogućuje taj izbor. U tom smislu u članku 7. stavku 2. OUZP-a navodi se da zahtjev za privolu mora biti predočen na način da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz uporabu jasnog i jednostavnog jezika. Korisnici platformi društvenih medija mogu dati privolu za oglase ili posebne vrste analize tijekom postupka registracije i u kasnijoj fazi odabirom postavki zaštite podataka. U svakom slučaju, kako je istaknuto u uvodnoj izjavi 32. OUZP-a, privola se uvijek mora dati jasnom potvrdnom radnjom, tako da se unaprijed kvačicom označeno polje ili manjak aktivnosti korisnika ne smatraju privolom[26].

27. Kako je istaknuto u Smjernicama EDPB-a o privoli, da bi se privola smatrala „informiranom", korisnici moraju dobiti određenu minimalnu razinu informacija[27]. Ako se taj uvjet ne ispuni, privola pribavljena u postupku registracije ne može se smatrati valjanom na temelju OUZP-a, što znači da je obrada nezakonita.

28. Privola se od korisnika traži za razne svrhe (npr. daljnja obrada osobnih podataka). Privola nije posebna i zbog toga nije valjana ako korisnicima nisu jasno predočene i informacije o tome na što pristaju[28]. Kako je predviđeno člankom 7. stavkom 2. OUZP-a, privolu bi trebalo zatražiti na način da je se može jasno razlučiti od drugih informacija neovisno o tome kako se informacije predočuju ispitaniku. Konkretno, ako se privola traži elektroničkim putem, ne smije biti uvrštena među uvjete korištenja[29]. Uzimajući u obzir činjenicu da sve više korisnika pristupa platformama društvenih medija putem sučelja pametnih mobilnih uređaja radi registracije, pružatelji usluga društvenih medija moraju posebno voditi računa o načinu na koji se traži privola kako bi je se moglo razlučiti od drugih pitanja. Korisnike se ne smije izlagati prekomjernoj količini informacija zbog koje će odustati od čitanja. U suprotnom, ako su korisnici „obvezni" potvrditi da su pročitali sva pravila zaštite privatnosti i pristaju na uvjete pružatelja usluga društvenih medija, uključujući sve postupke obrade, kako bi mogli izraditi račun, to se može smatrati prisilnom privolom za navedene posebne uvjete. Ako odbijanje privole dovodi do uskraćivanja usluge, ne može se smatrati da je ona dobrovoljna, granularna i posebna kako je propisano u OUZP-u. Ako je privola „uključena" u prihvaćanje uvjeta pružatelja usluga društvenih medija, ne smatra se da je „dana dobrovoljno"[30]. To vrijedi i kad voditelj obrade „veže" odredbu ugovora ili uslugu uz zahtjev za privolu, pa tako obrađuje osobne podatke koji mu nisu nužni za izvršenje ugovora.

29. Privola se mora izraziti pozitivnom radnjom korisnika, a nepostojanje privole trebalo bi se smatrati zadanom pretpostavkom sve dok je korisnik ne izrazi. Korisnici stoga ne bi trebali biti obvezni poduzimati ikakve radnje kako bi izrazili odbijanje ili bi odbijanje trebalo biti jednako jednostavno kao davanje privole[31].

ii. Povlačenje privole – članak 7. stavak 3. OUZP-a

[25] Smjernice EDPB-a 5/2020 o privoli na temelju Uredbe 2016/679, verzija 1.1., donesene 4. svibnja 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_hr.pdf.
[26] Vidjeti presudu Suda Europske unije od 1. listopada 2019., *Verbraucherzentrale Bundesverband e.V. protiv Planet 49 GmbH*, predmet C-673/17, točke od 62. do 63.
[27] Smjernice 5/2020 o privoli, točka 64.; vidjeti i scenarij uporabe 3a u dijelu 3.3. ovih Smjernica.
[28] Vidjeti Smjernice 5/2020 o privoli, točku 68.
[29] Smjernice o transparentnosti, točka 8.
[30] Vidjeti Smjernice 8/2020 o ciljanju korisnika društvenih medija, točku 57.
[31] Vidjeti uvodnu izjavu 42. petu rečenicu OUZP-a.

30. U skladu s člankom 7. stavkom 3. prvom rečenicom OUZP-a korisnici platformi društvenih medija u svakom trenutku mogu povući svoju privolu. Prije davanja privole korisnici moraju biti upoznati i s pravom na njezino povlačenje, kako je propisano člankom 7. stavkom 3. trećom rečenicom OUZP-a. Voditelji obrade moraju dokazati da korisnici imaju mogućnost odbiti davanje privole ili je povući bez ikakvih posljedica. Korisnici platformi društvenih medija koji pristanu na obradu svojih osobnih podataka jednim klikom, na primjer označivanjem polja, trebaju moći povući svoju privolu na jednako jednostavan način[32]. Time se naglašava da bi privola trebala biti reverzibilna odluka kako bi ispitanik zadržao određeni stupanj nadzora nad obradom[33]. Jednostavno povlačenje privole preduvjet je valjane privole u skladu s člankom 7. stavkom 3. četvrtom rečenicom OUZP-a i trebalo bi biti moguće bez snižavanja razine usluge[34]. Na primjer, privola se ne može smatrati valjanom u skladu s OUZP-om ako se dobiva samo jednim klikom miša, povlačenjem prsta ili pritiskom tipke, ali je za njezino povlačenje potrebno više koraka[35], teže ga je izvršiti ili dulje traje.

c. Obmanjujući obrasci dizajna

31. Više odredaba OUZP-a odnosi se na postupak registracije. Postoji nekoliko obmanjujućih obrazaca dizajna koji se mogu pojaviti ako pružatelji usluga društvenih medija ne provode pravilno OUZP.

i. Obrasci koji se temelje na sadržaju

Preopterećenost – kontinuirano prikazivanje upita (Prilog I., kontrolni popis 4.1.1.)

32. ***Kontinuirano prikazivanje upita*** obmanjujući je obrazac dizajna koji se javlja kad se korisnike potiče da daju više osobnih podataka nego što je nužno za svrhu obrade ili da pristanu na drukčije korištenje njihovih podataka opetovanim prikazivanjem zahtjeva da daju dodatne podatke ili da pristanu na određenu svrhu obrade. Takvi opetovani upiti mogu se prikazivati na jednom ili više uređaja. Korisnici će vjerojatno popustiti jer ih iscrpljuje odbijanje zahtjeva pri svakom korištenju platforme.

Primjer 1:

Inačica A: U prvom koraku postupka registracije korisnici moraju birati između nekoliko mogućnosti registracije. Mogu unijeti e-adresu ili broj telefona. Ako korisnici odaberu e-adresu, pružatelj usluga društvenih medija i dalje ih nastoji nagovoriti da unesu broj telefona tvrdeći da će se koristiti za sigurnost računa a da pritom ne navodi alternativnu vrstu podataka koje bi korisnici mogli unijeti ili su ih već unijeli. Konkretno, za vrijeme postupka registracije pojavljuje se više prozora s poljem za broj telefona s objašnjenjem: „Koristit ćemo vaš [telefonski] broj za sigurnost računa." Iako korisnici mogu zatvoriti taj prozor, to ih prekomjerno opterećuje te popuštaju i navode svoj broj telefona.

Inačica B: Drugi pružatelj usluga društvenih medija opetovano traži od korisnika da navedu broj telefona pri svakoj prijavi u račun unatoč tome što su ga korisnici prethodno odbili dati u postupku registracije ili pri posljednjoj prijavi.

[32] Vidjeti Smjernice o transparentnosti, točku 113. i dalje.
[33] Smjernice 5/2020 o privoli, točka 10.
[34] Smjernice 5/2020 o privoli, točka 114.
[35] Vidjeti Smjernice 5/2020 o privoli, točku 114.

33. U gornjem primjeru opisana je situacija u kojoj se od korisnika kontinuirano traži da navedu određene osobne podatke, na primjer broj telefona. Dok se u inačici A primjera to ***kontinuirano prikazivanje upita*** događa više puta u postupku registracije, inačica B pokazuje da se korisnici s tim obmanjujućim obrascem dizajna mogu suočiti i nakon registracije. Da bi se izbjegao taj obmanjujući obrazac dizajna, važno je posebno voditi računa o načelima smanjenja količine podataka u skladu s člankom 5. stavkom 1. točkom (c) OUZP-a, a u slučajevima kao u inačici A primjera 1 i o načelu ograničavanja svrhe u skladu s člankom 5. stavkom 1. točkom (b) OUZP-a. Stoga, kad pružatelji usluga društvenih medija navedu da će broj telefona koristiti „za sigurnost računa", smiju ga obrađivati samo u navedene sigurnosne svrhe i ne smiju nikakvom daljnjom obradom prekoračiti tu prvotnu svrhu.

34. Kako bi se poštovalo načelo smanjenja količine podataka, pružatelji usluga društvenih medija ne smiju tražiti dodatne podatke, na primjer broj telefona, ako su podaci koje su korisnici već naveli u postupku registracije dostatni. Na primjer, da bi se zaštitio račun, moguće je obaviti poboljšanu autentifikaciju bez broja telefona jednostavnim slanjem koda na račune e-pošte korisnika ili na druge načine.

35. Pružatelji usluga društvenih mreža stoga bi trebali primjenjivati sigurnosne značajke koje korisnici mogu jednostavnije ponovno pokrenuti. Na primjer, pružatelj usluga društvenih medija može korisnicima poslati broj za autentifikaciju dodatnim komunikacijskim kanalom, kao što je sigurnosna aplikacija koju su korisnici prethodno instalirali na svoj mobilni telefon, a da se pritom od korisnika ne traži broj mobilnog telefona. Isto tako, autentifikacija korisnika e-adresom manje je nametljiva od traženja broja telefona jer korisnici mogu jednostavno stvoriti novu e-adresu posebno za postupak registracije i uglavnom je koristiti za tu društvenu mrežu. Međutim, broj telefona nije tako lako zamijeniti jer nije izgledno da će korisnici kupiti novu SIM karticu ili sklopiti novi ugovor o telefonskim uslugama samo radi autentifikacije.

36. Treba imati na umu da se, ako je cilj takvog zahtjeva dokazati da korisnici legitimno posjeduju uređaj kojim se prijavljuju na društvenu mrežu, on može postići na više načina, a broj telefona samo je jedan od njih. Broj telefona stoga može biti samo jedna od relevantnih dobrovoljnih opcija za korisnike. Naposljetku, korisnici moraju odlučiti žele li koristiti to sredstvo kao faktor autentifikacije. Konkretno, za jednokratnu provjeru nije potreban broj telefona korisnika jer je e-adresa stalna točka za kontakt s korisnicima u postupku registracije.

37. Praksa opisana u inačici A primjera 1 može zavarati korisnike i navesti ih da daju takve informacije protiv svoje volje jer misle da je to potrebno za aktivaciju ili zaštitu računa. Međutim, zapravo se korisnicima nikad ne nudi alternativna opcija (npr. korištenje e-adrese za aktivaciju računa i u sigurnosne svrhe). U inačici B primjera 1 korisnici nisu obaviješteni o svrsi obrade. Međutim, ta inačica i dalje je obmanjujući obrazac dizajna poznat kao ***kontinuirano prikazivanje upita*** jer pružatelj usluga društvenih medija ne uvažava činjenicu da su korisnici već odbili navesti broj telefona te ga i dalje traži. Ako korisnici steknu dojam da mogu izbjeći ponavljanje zahtjeva isključivo unosom svojih podataka, vjerojatno će popustiti.

38. U sljedećem primjeru korisnike se opetovano potiče da platformi društvenih medija omoguće pristup svojim kontaktima:

Primjer 2: Platforma društvenih medija prikazuje znak za informacije ili upitnik kako bi potaknula korisnike da izvrše „neobveznu" radnju koja se traži u tom trenutku. Međutim, umjesto da samo pruži informacije korisnicima koji očekuju da će klikom na taj gumb dobiti pomoć, platforma ih potiče da prihvate uvoz kontakata s njihova računa e-pošte opetovanim prikazivanjem skočnog prozora s natpisom „Učinimo to".

39. Osobito u fazi registracije ***kontinuirano prikazivanje upita*** može navesti korisnike da prihvate zahtjev platforme kako bi konačno dovršili postupak. Učinak tog obmanjujućeg obrasca dizajna jači je u kombinaciji s motivacijskim jezikom kao u ovom primjeru, koji stvara osjećaj hitnosti.

40. Utjecaj teksta i vizualnih prikaza dodatno će se razmotriti u opisu obmanjujućeg uzorka dizajna poznatog kao ***upravljanje emocijama*** u nastavku[36].

Ometanje – zavaravajuća radnja (Prilog I., kontrolni popis 4.4.3.)

41. Još jedan primjer situacije u kojoj pružatelji usluga društvenih medija bez potrebe traže broj telefona korisnika odnosi se na korištenje aplikacije platforme:

Primjer 3: Pri registraciji na platformu društvenih medija preglednikom na računalu korisnicima se preporučuje da koriste i mobilnu aplikaciju platforme. Korisnike se poziva da istraže aplikaciju, što se čini kao još jedan korak u postupku registracije. Kad kliknu na ikonu očekujući da će ih se preusmjeriti u trgovinu aplikacija, umjesto toga od njih se traži da navedu svoj broj kako bi primili SMS poruku s poveznicom na aplikaciju.

42. Objašnjenje korisnicima da trebaju navesti broj telefona kako bi dobili poveznicu za preuzimanje aplikacije primjer je ***zavaravajuće radnje*** iz više razloga: prvo, aplikacije se mogu koristiti na više načina, npr. skeniranjem QR koda, klikom na poveznicu ili preuzimanjem aplikacije iz trgovine aplikacija. Drugo, te alternative pokazuju da ne postoji obvezan razlog da pružatelj usluge društvene platforme traži broj telefona korisnika. Nakon što korisnici dovrše postupak registracije, moraju se moći prijaviti uz pomoć svojih podataka za prijavu (obično su to e-adresa i lozinka) bez obzira na to koji uređaj koriste i koriste li preglednik na računalu odnosno mobilnom telefonu ili aplikaciju. To je još važnije i zbog činjenice da bi umjesto na pametni telefon korisnici mogli poželjeti instalirati aplikaciju na tablet, koji nije povezan s brojem telefona.

Stimuliranje – upravljanje emocijama (Prilog I., kontrolni popis 4.3.1.)

43. Obmanjujući obrazac dizajna ***upravljanje emocijama*** podrazumijeva da se tekstom ili vizualnim elementima (stil, boje, slike ili drugo) informacije predstavljaju korisnicima na vrlo pozitivan način, zbog čega se oni osjećaju dobro, sigurno ili nagrađeno, ili na vrlo negativan način, zbog čega se osjećaju tjeskobno, krivo ili kažnjeno. Način na koji se informacije prikazuju korisnicima utječe na njihovo emocionalno stanje i vjerojatno će ih potaknuti da postupe protivno svojim interesima u području zaštite podataka. Takve prakse mogu biti još učinkovitije ako se temelje na podacima koje je prikupila platforma. Utjecanje na odluke pružanjem pristranih informacija pojedincima općenito se može smatrati nepoštenom praksom koja je u suprotnosti s načelom poštenosti obrade utvrđenim u članku 5. stavku 1. točki (a) OUZP-a. Do toga može doći tijekom cijelog korisničkog putovanja na platformi društvenih medija. Međutim, u fazi registracije učinak upravljanja može biti posebno jak jer su korisnici uz korake potrebne za dovršetak registracije opterećeni velikom količinom informacija.

44. U kontekstu navedenog ***upravljanje emocijama*** u fazi registracije na platformi društvenih medija može još više utjecati na djecu, starije osobe i druge skupine (koje mogu pružiti više osobnih podataka zbog nerazumijevanja aktivnosti obrade) s obzirom na to da je riječ o ranjivim ispitanicima[37]. Ako su usluge

[36] Vidjeti točku 43. i dalje u scenariju uporabe 1, kao i pregled primjera u kontrolnom popisu u Prilogu.
[37] Vidjeti i točku 7.

platformi društvenih medija namijenjene djeci ili drugim ranjivim ispitanicima, trebale bi koristiti primjereni jezik, uključujući ton i stil, kako bi ranjivi korisnici kao primatelji poruke lako razumjeli pružene informacije[38]. S obzirom na ranjivost djece, starijih osoba i drugih ispitanika, zbog utjecaja obmanjujućih obrazaca dizajna i „zapovjednih" izraza koji se u njima koriste ti korisnici mogu se osjećati primoranima da podijele više informacija, na primjer kako bi bili omiljeni među vršnjacima ili jer smatraju da je davanje podataka obvezno.

45. Kad se od korisnika platformi društvenih medija traži da brzo daju svoje podatke, oni nemaju vremena da „obrade" i stvarno razumiju pružene informacije kako bi donijeli svjesnu odluku. Motivacijski jezik kojim se koriste platforme društvenih medija mogao bi potaknuti korisnike da dijele više podataka nego što je potrebno ako smatraju da će većina korisnika prihvatiti prijedlog platforme društvenih medija i da je to „pravilno" postupanje.

> **Primjer 4:** Platforma društvenih medija sljedećim tekstom traži od korisnika da podijele svoju geolokaciju: „Baš si samotnjak, zar ne? Ali dijeljenje i povezivanje s drugima čini svijet boljim mjestom! Podijeli svoju geolokaciju! Neka te mjesta i ljudi oko tebe nadahnu!"

46. Za vrijeme postupka registracije cilj je korisnika dovršiti registraciju kako bi mogli koristiti platformu društvenih medija. Obmanjujući obrasci dizajna kao što je ***upravljanje emocijama*** imaju jači učinak u tom kontekstu. Postoji rizik da će on biti izraženiji u sredini ili prema kraju postupka registracije u odnosu na početak jer se korisnici uglavnom žure dovršiti preostale korake ili su podložniji osjećaju hitnosti. U tom je kontekstu vjerojatnije da će korisnici pristati podijeliti sve podatke koji se od njih traže a da se pritom neće zapitati bi li to trebali učiniti. U tom smislu motivacijski jezik kojim se koristi pružatelj usluga društvenih medija može utjecati na trenutnu odluku korisnika, kao i kombinacija motivacijskog jezika i drugih oblika naglašavanja, na primjer uskličnika, kako je prikazano u primjeru u nastavku.

> **Primjer 5:** Pružatelj usluga društvenih medija potiče korisnike da podijele više osobnih podataka nego što je stvarno potrebno tako što od njih traži da se opišu: „Podijelite svoju sjajnu osobnost s nama! Zaista nas zanima, zato ne odugovlačite i odmah nam javite!"

47. Takvom praksom platforme društvenih medija dobivaju detaljniji profil svojih korisnika. Međutim, ovisno o slučaju, davanje više osobnih podataka, npr. o osobnosti korisnika, možda neće biti nužno za korištenje same usluge i stoga je riječ o kršenju načela smanjenja količine podataka u skladu s člankom 5. stavkom 1. točkom (c) OUZP-a. Kako je prikazano u primjeru 5, takve tehnike ne pogoduju ostvarivanju slobodne volje korisnika pri davanju podataka. Autoritativni jezik korisnicima može izazvati osjećaj obveze da unesu vlastiti opis jer su već uložili vrijeme u registraciju i žele je dovršiti. U postupku registracije računa manje je vjerojatno da će korisnici razmisliti o tome kakav će opis unijeti ili čak žele li ga uopće unijeti. To se ponajviše odnosi na slučajeve kad je tekst sročen tako da stvara osjećaj hitnosti ili zvuči kao zapovijed. Ako korisnici osjećaju tu obvezu čak i ako davanje podataka zapravo nije obvezno, to može utjecati na njihovu „slobodnu volju". To znači i da su informacije koje je pružila platforma društvenih medija bile nejasne.

> **Primjer 6:** Dio postupka registracije u kojem se od korisnika traži da učitaju svoju sliku sadržava gumb sa znakom „?". Klikom na njega prikazuje se sljedeća poruka: „Nema potrebe da prvo idete na frizuru. Samo odaberite fotografiju koja poručuje: ‚Ovo sam ja.'""

48. Čak i ako je cilj rečenica u primjeru 6 motivirati korisnike i naizgled pojednostavniti postupak u njihovu korist (tj. za registraciju nije potrebna formalna fotografija), takva praksa može utjecati na konačnu

[38] Vidjeti Smjernice o transparentnosti, točku 18.

odluku korisnika koji su prvotno odlučili da neće dijeliti fotografiju za svoj račun. Upitnik se koristi za postavljanje pitanja, a kad ga korisnici vide na ikoni, očekuju da će klikom na nju dobiti korisne informacije. Ako se to očekivanje ne ostvari i korisnike se umjesto toga ponovno potiče na radnju koju oklijevaju poduzeti, privola prikupljena bez obavješćivanja korisnika o obradi njihove slike ne bi bila valjana jer ne bi bio ispunjen zahtjev o „informiranoj" i „dobrovoljnoj" privoli u skladu s člankom 7. OUZP-a u vezi s člankom 4. točkom 11. OUZP-a. Aspekt emocija stoga uvelike utječe na legitimitet privole.

Ometanje – dulje trajanje nego što je nužno (Prilog I., kontrolni popis 4.4.2.)

49. Kad korisnici pokušaju aktivirati kontrolu povezanu sa zaštitom podataka, ali je korisničko putovanje osmišljeno tako da je za to potrebno više koraka nego za aktivaciju opcija invazivnih za podatke, riječ je o obmanjujućem uzorku dizajna poznatom kao ***dulje trajanje od nužnog***. Taj obrazac vjerojatno će odvratiti korisnike od aktivacije kontrola za zaštitu podataka. U postupku registracije može se prikazati skočni prozor u kojem se od korisnika traži da potvrde svoju odluku kad odaberu restriktivnu opciju (npr. ako odaberu postaviti profil kao privatan). U primjeru u nastavku opisan je još jedan slučaj postupka registracije koji traje ***dulje nego što je nužno.***

Primjer 7: Tijekom postupka registracije korisnicima koji kliknu na gumbe „preskoči" kako bi izbjegli unos određene vrste podataka prikazuje se skočni prozor s pitanjem: „Jeste li sigurni?" Propitivanjem i izazivanjem sumnje u odluku pružatelj usluga društvenih medija potiče korisnike da je preispitaju i unesu tražene vrste podataka, kao što su spol, popis kontakata ili fotografija. Suprotno tomu, korisnicima koji odluče izravno unijeti podatke ne prikazuje se poruka koja ih potiče da preispitaju svoj izbor.

U ovom primjeru, ako se od korisnika traži da potvrde da ne žele unijeti podatke, oni se mogu predomisliti i unijeti tražene podatke. To se posebno odnosi na korisnike koji nisu upoznati s načinom rada predmetne platforme društvenih medija. Obmanjujućim obrascem dizajna ***dulje trajanje od nužnog*** nastoji se utjecati na odluke korisnika tako što ih se zadržava i dovodi u pitanje njihov početni izbor, dok se ujedno nepotrebno produljuje postupak registracije, čime se krši načelo poštenosti iz članka 5. stavka 1. točke (a) OUZP-a. Primjer pokazuje da obmanjujući obrazac dizajna može navesti korisnike da otkriju više osobnih podataka nego što su prvotno odabrali. Opisana je neravnoteža u postupanju prema korisnicima koji odmah otkriju osobne podatke i onima koji to ne učine: samo se od onih koji odbiju otkriti podatke traži da potvrde svoj izbor, dok se od korisnika koji te podatke otkriju ne traži potvrda. Time se krši načelo poštenosti iz članka 5. stavka 1. točke (a) OUZP-a s obzirom na korisnike koji ne žele otkriti te osobne podatke.

ii. Obrasci koji se temelje na sučelju

Stimuliranje – skrivanje na vidljivom mjestu (Prilog I., kontrolni popis 4.3.2.)

50. U skladu s načelom transparentnosti ispitanicima se na jasan način moraju pružiti informacije da bi razumjeli kako se njihovi osobni podaci obrađuju i kako ih mogu nadzirati. Osim toga, te informacije moraju biti lako uočljive ispitanicima. Međutim, informacije povezane sa zaštitom podataka, osobito poveznice, često su prikazane tako da ih korisnici lako previde. U okviru prakse ***skrivanja na vidljivom mjestu*** za informacije ili kontrole zaštite podataka koristi se vizualni stil kojim se korisnike

preusmjerava s opcija koje pogoduju zaštiti podataka prema manje restriktivnim, a time i invazivnijim opcijama.

51. Korištenje male veličine slova ili boje koja je nedovoljno kontrastna da bi se omogućila dostatna čitljivost (npr. bljedosivi tekst na bijeloj pozadini) može negativno utjecati na korisnike jer će tekst biti manje vidljiv i korisnici će ga previdjeti ili će imati poteškoća s čitanjem. To se posebno odnosi na situacije u kojima se pored obveznih informacija povezanih sa zaštitom podataka nalazi jedan ili više upadljivih elemenata. Te tehnike oblikovanja sučelja zavaravaju korisnike te otežavaju i produljuju prepoznavanje informacija povezanih sa zaštitom njihovih podataka jer je potrebno više vremena i temeljitosti da bi se uočile relevantne informacije.

Primjer 8: Čim dovrše registraciju, korisnici mogu pristupiti informacijama o zaštiti podataka samo ako otvore opći izbornik platforme društvenih medija i pretraže odjeljak podizbornika koji sadržava poveznicu na „postavke privatnosti i podataka". Kad se stranica otvori, poveznica na pravila zaštite privatnosti nije vidljiva na prvi pogled. Korisnici moraju primijetiti sićušnu ikonu u kutu stranice koja vodi do pravila zaštite privatnosti, što znači da im je teško uočiti gdje se nalaze informacije o pravilima zaštite podataka.

52. Važno je napomenuti da, čak i kad pružatelji usluga društvenih medija stave na raspolaganje sve informacije koje treba pružiti ispitanicima u skladu s člancima 13. i 14. OUZP-a, načinom prikazivanja tih informacija svejedno mogu kršiti sveobuhvatne zahtjeve transparentnosti iz članka 12. stavka 1. OUZP-a. Ako su informacije ***skrivene na vidljivom mjestu***, zbog čega će ih se vjerojatno previdjeti, to dovodi do zabune ili dezorijentiranosti te se ne može smatrati da su one razumljive i lako dostupne, što je u suprotnosti s člankom 12. stavkom 1. OUZP-a.

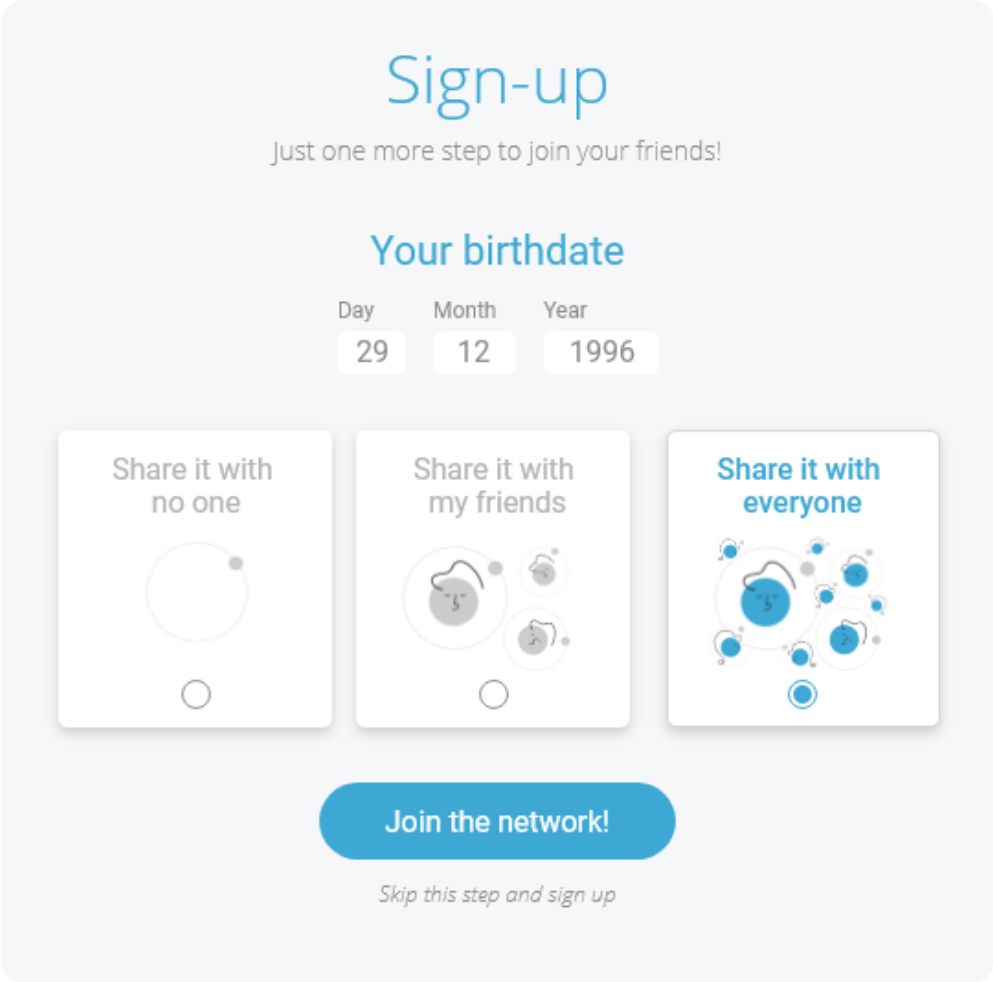
53. Iako se u gornjem primjeru opisuje obmanjujući obrazac dizajna nakon postupka registracije, on se pojavljuje i za vrijeme tog postupka, kao što će se prikazati u primjeru u nastavku, u kojem se kombiniraju obrasci ***skrivanje na vidljivom mjestu*** i ***obmanjujući komfor***.

Preskakanje – obmanjujući komfor (Prilog I., kontrolni popis 4.2.1.)

54. Pružatelji usluga društvenih medija moraju voditi računa i o načelu integrirane zaštite podataka. Ako su postavke podataka unaprijed odabrane, korisnici uživaju posebnu razinu zaštite podataka koju automatski utvrđuje pružatelj usluga, a ne korisnici. Osim toga, korisnicima nije uvijek dostupna opcija da odmah odaberu strože postavke u skladu sa zahtjevima zaštite podataka. U tom smislu usklađenost s OUZP-om ne znači da sve opcije moraju biti potpuno jednake. Međutim, ako pružatelji usluga društvenih medija istaknu jednu od opcija i tako korisnicima skrenu pozornost na nju, to mora biti najrestriktivnija opcija u smislu osobnih podataka kako bi se, među ostalim, zadovoljilo načelo smanjenja količine podataka u skladu s člankom 5. stavkom 1. točkom (c) OUZP-a.

55. Ako su automatski omogućene značajke i opcije najinvazivnije za podatke, riječ je o obrascu ***obmanjujući komfor***. Zbog učinka zadanih postavki koji potiče pojedince da zadrže unaprijed odabranu opciju nije vjerojatno da će ih korisnici promijeniti čak i ako im se za to pruži mogućnost. Ta je praksa česta u postupcima registracije, kako je prikazano u primjeru 9 u nastavku, jer se njome učinkovito aktiviraju invazivne opcije za podatke koje bi korisnici inače vjerojatno odbili. Takvi obmanjujući obrasci dizajna protivni su načelu integrirane zaštite podataka iz članka 25. stavka 2. OUZP-a, posebno kad

utječu na prikupljanje osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost[39].



Primjer 9: Kad korisnici unesu svoj datum rođenja, poziva ih se da odaberu s kim će dijeliti tu informaciju. Iako su dostupne manje invazivne mogućnosti, automatski je odabrana opcija „podijeli sa svima", što znači da će svi, tj. registrirani korisnici i svi korisnici interneta, moći vidjeti korisnikov datum rođenja.

56. U primjeru 9 opisan je obrazac ***obmanjujući komfor*** jer prema zadanim postavkama nije odabrana, a stoga ni aktivirana, opcija koja nudi najvišu razinu zaštite podataka. Osim toga, zbog učinka zadanih postavki tog obrasca korisnici će vjerojatno zadržati automatski odabrane postavke, odnosno neće u trenutačnoj fazi razmatrati druge opcije niti će se kasnije vratiti na postavku i izmijeniti je. U predmetnom sučelju koristi se i obrazac ***skrivanje na vidljivom mjestu***. Naime, unos datuma rođenja nije obvezan jer korisnici mogu preskočiti taj korak registracije klikom na poveznicu „Preskoči ovaj korak i registriraj se", koja se nalazi ispod gumba „Pridruži se mreži!". Budući da su polje za datum rođenja i gumb za potvrdu jako istaknuti, korisnici će vjerojatno unijeti datum rođenja i poslati ga

[39] Vidjeti i točku 446. Konačne odluke irskog tijela za zaštitu podataka o Instagramu (Meta Platforms Ireland Limited) nakon obvezujuće odluke EDPB-a o rješavanju sporova od 28. srpnja 2022., https://www.edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_hr.

društvenoj mreži jer ne primjećuju da je moguće uskratiti tu informaciju. Taj bi učinak bio još jači kad bi se uz polje i gumb prikazivali animirani krugovi koji bi izrazito privukli pozornost korisnika.

57. Poštovanje načela tehničke i integrirane zaštite podataka ne podrazumijeva da sve ponuđene opcije moraju biti potpuno jednake. Međutim, ako voditelji obrade odluče istaknuti samo jednu među više opcija, trebali bi istaknuti onu najrestriktivniju u smislu obrade podataka.

58. Osim što potiču korisnike da zadrže opciju koja ne odgovara nužno njihovim preferencijama, pružatelji usluga društvenih medija možda neće uputiti korisnike da provjere ili izmijene postavke zaštite podataka u skladu sa svojim preferencijama kad dovrše postupak registracije. Štoviše, za promjenu zadanih postavki možda će biti potrebno više koraka. Ako se od korisnika ni na koji način ne zatraži da provjere ili izmijene svoje postavke zaštite podataka ili ih se jasno ne uputi na povezane informacije, njihova razina zaštite podataka ovisit će o njihovoj osobnoj inicijativi. Kako bi se korisnicima olakšao nadzor njihovih podataka, dostupne su takozvane nadzorne ploče za privatnost, predviđene za centralizaciju i pojednostavnjenje nadzora.

59. Važno je imati na umu da nedostatna tehnička i integrirana zaštita podataka u kombinaciji s navedenim učinkom zadanih postavki može ostaviti štetne posljedice za ispitanike, među ostalim za njihovu kibersigurnost. Objavljivanje osobnih podataka, na primjer datuma rođenja, na temelju kojih druge internetske usluge provode postupke provjere, kriminalcima bi moglo olakšati pristup računima korisnika za kupnju te bankovnim i drugim računima. Još jedna štetna posljedica odnosi se na mogućnosti stupanja u kontakt na platformi društvenih medija: ako je zadana opcija za slanje zahtjeva za kontakt ili poruka korisnicima postavljena na „bilo tko”, to povećava rizik od mamljenja na internetu i prijevara, posebno za ranjive skupine.

60. Naposljetku, ako se ***obmanjujući komfor*** primijeni na prikupljanje privole, što bi podrazumijevalo da se automatski pretpostavlja da korisnik daje privolu, na primjer unaprijed označenim poljem ili tumačenjem neaktivnosti kao odobrenje, uvjeti za privolu utvrđeni u članku 4. točki 11. OUZP-a nisu ispunjeni i obrada bi se smatrala nezakonitom u skladu s člankom 5. stavkom 1. točkom (a) i člankom 6. stavkom 1. točkom (a) OUZP-a.

Ometanje – slijepa ulica (Prilog I., kontrolni popis 4.4.1.)

61. Važno je istaknuti da je faza registracije ključni trenutak za informiranje korisnika. Ako traže informacije i ne mogu ih pronaći jer poveznica za preusmjeravanje nije dostupna ili ne funkcionira, riječ je o obrascu ***slijepa ulica*** jer korisnici ne mogu ostvariti taj cilj.

Primjer 10: Nakon pokretanja postupka registracije korisnici ne dobivaju poveznice na informacije o zaštiti podataka. Korisnici ne mogu pronaći te informacije jer nisu navedene na sučelju za registraciju, čak ni u njegovu podnožju.

62. U praksi taj primjer podrazumijeva da korisnici mogu samo zaustaviti registraciju i vratiti se na početnu stranicu ako ona sadržava poveznicu na obavijest o zaštiti privatnosti ili dovršiti registraciju, prijaviti se na platformu društvenih medija i tek tada ostvariti pristup informacijama o zaštiti podataka. Time se krši načelo transparentnosti i lake dostupnosti informacija koje se pružaju ispitanicima u skladu s člankom 12. stavkom 1. OUZP-a. Osim toga, nije u skladu sa zahtjevima iz članka 13. stavaka 1. i 2. OUZP-a jer se u trenutku prikupljanja osobnih podataka ne dostavljaju informacije i ne može im se pristupiti.

63. Obrazac ***slijepa ulica*** može se manifestirati i drukčije, ako se korisnicima u postupku registracije omogući radnja ili opcija povezana sa zaštitom podataka koju ne mogu pronaći kasnije, dok koriste uslugu.

> **Primjer 11:** Za vrijeme postupka registracije korisnici mogu dati privolu za obradu svojih osobnih podataka u svrhu oglašavanja te ih se obavještava da svoj izbor mogu promijeniti u bilo kojem trenutku nakon registracije na društvenom mediju otvaranjem pravila zaštite privatnosti. Međutim, nakon što korisnici dovrše postupak registracije i otvore pravila zaštite privatnosti, ne mogu pronaći način ili upute za povlačenje privole za tu obradu.

64. U ovom konkretnom primjeru korisnici nemaju kako povući privolu nakon registracije. Obmanjujućim obrascem dizajna poznatim kao ***slijepa ulica*** krši se pravo ispitanika na povlačenje privole u bilo kojem trenutku, koje mora biti jednako jednostavno kao i njezino davanje, u skladu s člankom 7. stavkom 3. prvom i četvrtom rečenicom OUZP-a.

65. Naposljetku, i upućivanje korisnika na poveznicu koja ih navodno vodi do stranica povezanih sa zaštitom podataka, kao što su stranice s postavkama ili informacijama o zaštiti podataka, primjer je obrasca ***slijepa ulica*** ako poveznica nije valjana, a nisu dostupne zamjenske poveznice s pomoću kojih bi korisnici pronašli ono što traže. U toj situaciji korisnici ne mogu tražiti relevantne informacije i ne navodi im se nikakvo objašnjenje, na primjer zašto se to događa (npr. zbog tehničkih problema). U tom slučaju javljaju se problemi povezani s transparentnošću i jednostavnim pristupom informacijama kako su opisani u točki 58.

d. Primjeri dobre prakse

Kako bi dizajn korisničkih sučelja olakšao učinkovitu provedbu OUZP-a, EDPB preporučuje da se u postupak registracije uvedu sljedeći primjeri dobre prakse:

Prečaci: poveznice na informacije, radnje ili postavke koje korisnicima mogu olakšati upravljanje njihovim podacima i postavkama zaštite podataka trebale bi biti dostupne svaki put kad korisnici naiđu na povezane informacije ili iskustvo (*npr. poveznice na relevantne dijelove pravila zaštite privatnosti*).

Podaci za kontakt: u pravilima zaštite privatnosti trebala bi biti jasno navedena adresa poduzeća za slanje zahtjeva povezanih sa zaštitom podataka. Trebala bi se nalaziti u odjeljku u kojem je korisnici mogu očekivati, kao što su odjeljak o identitetu voditelja obrade, odjeljak o pravima ili odjeljak s podacima za kontakt.

Obraćanje nadzornom tijelu: konkretno imenovanje nadzornog tijela uz poveznicu na njegove internetske stranice ili posebne internetske stranice za podnošenje prigovora. Te bi informacije trebale biti navedene u odjeljku u kojem ih korisnici mogu očekivati, kao što je odjeljak o pravima.

Pregled pravila zaštite privatnosti: na početku/vrhu pravila zaštite privatnosti treba navesti sadržaj s naslovima i podnaslovima (koji se može sakriti i prikazati po želji) s prikazom odlomaka iz obavijesti o zaštiti privatnosti. Nazivi pojedinih odlomaka jasno usmjeravaju korisnike prema konkretnom sadržaju i omogućuju im da brzo prepoznaju i otvore odjeljak koji traže.

Praćenje promjena i usporedba: ako se u obavijest o zaštiti privatnosti unesu izmjene, trebaju biti dostupne prethodne verzije s datumom objave i istaknutim izmjenama.

Usklađeni tekst: na internetskim stranicama koristi se isti tekst i definicija za istu vrstu zaštite podataka. Tekst naveden u pravilima zaštite privatnosti trebao bi odgovarati tekstu na ostatku platforme.

Navođenje definicija: kad koristite nepoznate ili tehničke riječi ili izraze, navođenje definicije jednostavnim jezikom pomoći će korisnicima da razumiju pružene informacije. Definicija se može nalaziti izravno u tekstu, pojaviti se kad korisnici zadrže pokazivač miša iznad odgovarajuće riječi ili biti dostupna u pojmovniku.

Isticanje elemenata zaštite podataka: vizualno upečatljiv prikaz elemenata ili radnji povezanih sa zaštitom podataka na sučelju koje nije izravno posvećeno predmetnoj temi. Na primjer, pri dijeljenju javnog sadržaja na platformi kontrole za povezivanje geolokacije trebale bi biti izravno dostupne i jasno vidljive.

Uvod u zaštitu podataka: odmah nakon izrade računa pružatelj usluga društvenih medija treba u uvodnu fazu njihova korištenja uvrstiti elemente zaštite podataka kako bi korisnicima omogućio da bez teškoća prouče i prilagode svoje preferencije. Na primjer, može ih se pozvati da prilagode svoje preferencije zaštite podataka nakon što dodaju prvog prijatelja ili podijele prvu objavu.

Korištenje primjera: osim obveznih informacija u kojima se jasno i precizno navodi svrha obrade, određena vrsta obrade podataka može se ilustrirati primjerima kako bi je korisnici lakše razumjeli.

Kontekstualne informacije: osim iscrpnih pravila zaštite privatnosti treba navesti kratke informacije u najprikladnijem trenutku kako bi korisnik raspolagao konkretnim i stalnim informacijama o načinu obrade njegovih podataka.

3.2. Informiranje na društvenim medijima

Scenarij uporabe 2a: slojevita obavijest o zaštiti privatnosti

a. **Opis konteksta**

66. Kao što je već istaknuto u Smjernicama o transparentnosti, načelo transparentnosti vrlo je usko povezano s načelom poštene obrade osobnih podataka[40]. Međutim, pružanje informacija o obradi osobnih podataka potiče voditelje obrade da promišljaju svoje postupke, olakšava ispitanicima razumijevanje obrade podataka i, naposljetku, omogućuje im da nadziru svoje podatke, ponajprije ostvarivanjem svojih prava. Time se izjednačuju ovlasti uključenih osoba i uspostavlja se pošten sustav obrade osobnih podataka. Međutim, pružanje veće količine informacija ne znači da su te informacije nužno bolje. Previše nevažnih ili zbunjujućih informacija može prikriti važne elemente sadržaja ili otežati njihovo pronalaženje. U tom je području stoga ključna ravnoteža između sadržaja i razumljive prezentacije. Ako se ona ne postigne, mogu se pojaviti obmanjujući obrasci dizajna.

b. **Relevantne pravne odredbe**

67. Opisani odnosi postaju jasni na temelju članka 5. OUZP-a. Transparentnost i poštenost već se sustavno spominju zajedno u članku 5. stavku 1. točki (a) OUZP-a jer jedna sastavnica određuje drugu. Prema zahtjevu pouzdanosti iz članka 5. stavka 2. OUZP-a jasno je i da je nužna ne samo vanjska nego i unutarnja transparentnost. Najvažniji je element unutarnje transparentnosti obveza vođenja evidencije aktivnosti obrade u skladu s člankom 30. OUZP-a. Radi vanjske transparentnosti pružatelji usluga društvenih medija mogu korisnicima, među ostalim sredstvima informiranja, dostaviti slojevitu obavijest o zaštiti privatnosti[41]. Ta potreba za razumljivošću i poštenom obradom dovodi i do zahtjeva iz članka 12. stavka 1. OUZP-a, u kojem se navodi da se sve informacije iz članaka 13. i 14. OUZP-a pružaju u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika. Sadržaj informacija zato mora biti dostupan bez ikakvih prepreka. Ako nisu

[40] Smjernice o transparentnosti, str. 4–5.
[41] Vidjeti scenarij uporabe 2a u odjeljku 3.2. u nastavku.

ispunjeni zahtjevi iz članka 12. OUZP-a, ne postoje valjane informacije u smislu članaka 13. i 14. OUZP-a. Stoga se radi postizanja stvarnog nadzora voditelji obrade i izvršitelji obrade mogu smatrati odgovornima, što doprinosi praktičnoj djelotvornosti zahtjeva OUZP-a.

c. Obmanjujući obrasci dizajna

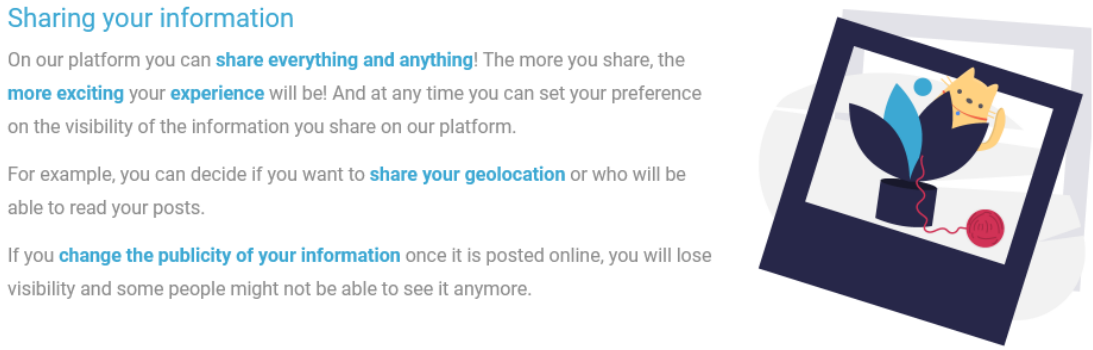
i. Obrasci koji se temelje na sadržaju

68. Kad je riječ o ovom scenariju uporabe, obrasci koji se temelje na sadržaju ograničeni su člankom 12. stavkom 1. OUZP-a, kojim se propisuje da se informacije pružaju u preciznom i razumljivom obliku te uz uporabu jasnog i jednostavnog jezika.

Držanje u neznanju – proturječne informacije (Prilog I., kontrolni popis 4.6.2.)

69. Jedan je od najočitijih primjera pružanje ***proturječnih informacija***, zbog kojih korisnici nisu sigurni kako bi trebali postupiti ni koje su posljedice njihovih postupaka, pa zato ne poduzimaju ništa ili zadržavaju zadane postavke.

70. Povrede u tom području, na primjer povreda članka 12. stavka 1. OUZP-a, mogu pogoršati drugi učinci kao što je ***upravljanje emocijama***. Motivirajući tekstovi, slike i boje, kao i privlačno oglašavanje, načelno su dopušteni. Međutim, vjerojatno će pojačati učinak obmanjujućih obrazaca dizajna, uključujući nepoštenu obradu u smislu članka 5. stavka 1. točke (a) OUZP-a.



Primjer 12: U ovom primjeru u informacijama o dijeljenju podataka obrada je prikazana iz vrlo pozitivne perspektive i ističu se prednosti dijeljenja što veće količine podataka. Zajedno s ilustracijom slatke životinje u igri s loptom ***upravljanje emocijama*** među korisnicima može stvoriti lažan osjećaj sigurnosti i komfora u vezi s mogućim rizicima dijeljenja određenih informacija na platformi. S druge strane, pružene informacije o tome kako nadzirati vidljivost vlastitih podataka nisu jasne. Prvo se navodi da korisnici u bilo kojem trenutku mogu prilagoditi preferencije dijeljenja. Međutim, iz zadnje rečenice proizlazi da to nije moguće nakon što je sadržaj već objavljen na platformi. Zbog tih ***proturječnih informacija*** korisnici nisu sigurni kako nadzirati objavu svojih podataka.

Nestalnost – nedostatak hijerarhije (Prilog I., kontrolni popis 4.5.1.)

71. Ako prikaz informacija nije u skladu s internim sustavom ili ikakvom hijerarhijom, mogu se pojaviti slični učinci kao u slučaju ***proturječnih informacija*** i ***upravljanja emocijama***. ***Nedostatak hijerarhije*** javlja se kad se informacije o zaštiti podataka pojavljuju više puta i prikazane su na više načina. Korisnike će taj višak informacija vjerojatno zbuniti i neće moći u potpunosti shvatiti kako se njihovi podaci obrađuju i kako ih nadzirati. Takva konfiguracija otežava razumijevanje informacija jer cjelovit pregled nije lako

dostupan. U slučajevima kao što je onaj iz sljedećeg primjera time se krše zahtjevi razumljivosti i lake dostupnosti iz članka 12. stavka 1. OUZP-a.

Primjer 13: Informacije koje se odnose na prava ispitanika navedene su u raznim dijelovima obavijesti o zaštiti privatnosti. Iako su prava ispitanika objašnjena u odjeljku „Vaše mogućnosti", pravo na podnošenje prigovora i točna adresa za kontakt spominju se tek nakon nekoliko odjeljaka i slojeva koji se odnose na druge teme. U obavijesti o zaštiti privatnosti djelomično nedostaju podaci za kontakt u fazama u kojima bi ih bilo poželjno i preporučljivo navesti.

72. ***Nedostatak hijerarhije*** može se pojaviti kad su informacije strukturirane tako da je korisnicima otežano snalaženje, kao što to pokazuje sljedeći primjer.

Primjer 14: Pravila zaštite privatnosti nisu podijeljena u odjeljke s naslovima i sadržajem. Sadržavaju više od 70 stranica. Međutim, ni na vrhu ni sa strane nema navigacijskog izbornika koji bi korisnicima omogućio jednostavan pristup traženom odjeljku. Samostalno osmišljeni pojam „podaci o izradi" objašnjen je u bilješci na stranici 67.

Držanje u neznanju – dvosmisleni tekst ili informacije (Prilog I., kontrolni popis 4.6.3.)

73. Čak i ako izbor riječi nije očigledno proturječan, problemi se mogu pojaviti zbog korištenja dvosmislenih i nejasnih pojmova pri davanju informacija korisnicima. Zbog takvih informacija korisnici vjerojatno neće biti sigurni kako će se podaci obrađivati ili kako ih mogu nadzirati. Ako se može pretpostaviti da prosječni korisnici koji ne raspolažu posebnim znanjem ne bi razumjeli stvarnu poruku informacija, uvjeti iz članka 12. stavka 1. OUZP-a nisu ispunjeni. Prema tome, korištenje ***dvosmislenog teksta ili informacija*** može biti u suprotnosti s načelom poštenosti iz članka 5. stavka 1. točke (a) OUZP-a jer se informacije ne mogu smatrati transparentnima, zbog čega ispitanici ne mogu razumjeti kako se obrađuju njihovi osobni podaci ni ostvariti svoja prava.

Primjer 15: U obavijesti o zaštiti privatnosti dio obrade opisan je nejasno i neprecizno, kao u sljedećoj rečenici: *Vaši podaci mogli bi se koristiti za poboljšanje naših usluga.* Osim toga, na obradu se primjenjuje pravo pristupa osobnim podacima na temelju članka 15. stavka 1. OUZP-a, ali ono se spominje tako da korisnicima nije jasno čemu mogu pristupiti: *Dio svojih podataka možete vidjeti na svojem računu i pregledom svojih objavi na platformi.*

74. Zbog uporabe kondicionala u primjeru („mogli bi") korisnici nisu sigurni hoće li se njihovi podaci koristiti za obradu. Pojam „usluge" vjerojatno je preopćenit da bi se smatrao „jasnim". Nije jasno ni kako će se podaci obrađivati radi poboljšanja usluga. EDPB podsjeća da kondicional ili nejasno formuliran tekst ne čine „jasan i jednostavan jezik" kako je propisano člankom 12. stavkom 1. prvom rečenicom OUZP-a i smiju se koristiti samo ako voditelji obrade mogu dokazati da se time ne dovodi u pitanje poštenost obrade[42].

Nestalnost – jezični diskontinuitet (Prilog I., kontrolni popis 4.5.4.)

[42] Vidjeti Smjernice o transparentnosti, točku 12., uključujući „Primjere loše prakse", i točku 13.

75. Kad se internetske usluge nude i pružaju stanovnicima određenih država članica, obavijesti o zaštiti podataka trebale bi biti dostupne i na tim jezicima[43]. U tom je kontekstu važno da se izbor određenog jezika može mijenjati i ručno te da se ta promjena odvija kontinuirano i bez prekida. Ako ti kriteriji nisu ispunjeni, ispitanici su izloženi ***jezičnom diskontinuitetu***, zbog čega ne mogu razumjeti informacije o zaštiti podataka. Korisnici će se susresti s tim obmanjujućim obrascem dizajna ako informacije o zaštiti podataka nisu navedene na nekom od službenih jezika zemlje u kojoj žive, a usluga se pruža na tom jeziku. Ako korisnici ne vladaju jezikom na kojem se pružaju informacije o zaštiti podataka, neće ih moći lako pročitati i zbog toga neće znati kako se njihovi osobni podaci obrađuju. Važno je napomenuti da ***jezični diskontinuitet*** može zbuniti korisnike i stvoriti okruženje postavki koje neće znati koristiti. Taj obmanjujući obrazac dizajna može se pojaviti u raznim oblicima, kao što će biti opisano u ovim Smjernicama.

Primjer 16:

Inačica A: Platforma društvenih medija dostupna je na hrvatskom jeziku po izboru korisnika (ili na španjolskom kao jeziku zemlje u kojoj se nalazi), ali su sve ili neke informacije o zaštiti podataka dostupne samo na engleskom jeziku.

Inačica B: Pri svakom otvaranju određenih stranica, kao što je stranica za pomoć, one se automatski prebacuju na jezik zemlje u kojoj se korisnik nalazi, čak i ako je prethodno odabrao drugi jezik.

76. Inačica A prikaz je slučaja u kojem informacije nisu dostupne na jeziku kojim ispitanik očito vlada. To znači da ne može pročitati informacije, a stoga ni razumjeti kako se obrađuju njegovi osobni podaci. Informacije se ne mogu smatrati razumljivima u smislu članka 12. stavka 1. OUZP-a. Budući da informacije o zaštiti podataka nisu dostupne na ispitanicima razumljivom jeziku, ne može se smatrati da su im pružene informacije propisane člankom 13. i člankom 14. OUZP-a.

77. U inačici B opisan je slučaj u kojem se stranice s informacijama o zaštiti podataka automatski prikazuju na jeziku zemlje boravišta korisnika unatoč tome što je korisnik jasno odabrao drugi jezik. To znači da pri svakom pristupanju stranici s informacijama o zaštiti podataka korisnici moraju ponovno postaviti željeni jezik. To se može smatrati nepoštenom praksom prema ispitanicima i moglo bi doprinijeti povredi načela poštenosti iz članka 5. stavka 1. točke (a) OUZP-a.

ii. Obrasci koji se temelje na sučelju

78. U nekim slučajevima pružatelji usluga društvenih medija primjenjuju posebnu praksu za prikaz svojih postavki zaštite podataka. U postupku registracije korisnicima se prikazuju brojne informacije i razne postavke povezane sa zaštitom podataka. Da bi korisnici mogli pronaći te postavke i izmijeniti ih u bilo kojem trenutku tijekom korištenja platforme, one bi trebale biti lako dostupne i povezane s relevantnim informacijama na temelju kojih bi mogli donijeti utemeljenu odluku. Element „lake dostupnosti" znači da ispitanici ne bi trebali sami tražiti predmetne informacije. Kad je riječ o pravilima zaštite privatnosti, Radna skupina iz članka 29. već je navela da se tekst ili poveznica koji su teško uočljivi zbog položaja ili sheme boja kojima su označeni ili koje je teško pronaći na internetskoj stranici ne smatraju lako dostupnima[44].

[43] Vidjeti Smjernice o transparentnosti, točku 13. i bilješku 15.
[44] Smjernice o transparentnosti, točka 11.

Preopterećenost – labirint pravila privatnosti (Prilog I., kontrolni popis 4.1.2.)

79. U skladu sa Smjernicama o transparentnosti obavijest o zaštiti privatnosti trebala bi biti lako dostupna, tj. jednim klikom na internetskim stranicama[45]. Primjena metode slojevitog pristupa može doprinijeti jasnijem prikazu obavijesti o zaštiti privatnosti u smislu članka 12. stavka 1. OUZP-a[46]. Međutim, taj pristup ne bi trebao uključivati složena pravila zaštite privatnosti koja se sastoje od brojnih slojeva jer bi to dovelo do pojave obmanjujućeg obrasca dizajna poznatog kao ***labirint pravila privatnosti***, koji bi otežao izvršavanje važnih funkcija i ostvarivanje prava. Taj obrazac otežava pronalaženje određene informacije ili kontrole zaštite podataka jer korisnici moraju otvarati niz stranica, a nije im dostupan sveobuhvatan i iscrpan pregled. Zbog toga će vjerojatno previdjeti relevantne informacije odnosno postavke ili odustati od potrage. Slojevit prikaz trebao bi olakšati čitljivost i pružiti informacije o ostvarivanju prava ispitanika, a ne otežati taj proces. Ključno je omogućiti korisnicima lako praćenje objašnjenja.

80. U tom smislu najbolji pristup za korisnike nije univerzalan i ovisi o nizu kriterija, na primjer o vrsti korisnika na platformi ili općenitoj vrsti dizajna aplikacije. Ako je moguće, primijenjeni slojeviti pristup trebalo bi testirati na korisnicima kako bi se dobile njihove povratne informacije i procijenila njegova učinkovitost. Zbog toga se ne može odrediti konkretan najveći dopušteni broj slojeva informacija. Zato se postojanje prevelikog broja slojeva koji dovode do pojave obmanjujućih obrazaca dizajna uvijek mora utvrđivati od slučaja do slučaja. Međutim, što je taj broj veći, to je vjerojatnije da će korisnici biti obeshrabreni ili dovedeni u zabludu. Velik broj slojeva prikladan je samo u posebnim slučajevima u kojima nije lako sveobuhvatno pružiti složene informacije. Isto tako, slojeviti pristup ne smije se zloupotrebljavati za skrivanje informacija u dubljim slojevima ili dodavanjem nepotrebnih slojeva.

81. Međutim, tom pitanju treba drukčije pristupiti kad je riječ o ostvarivanju prava korisnika. OUZP-om je propisano da ostvarivanje tih prava uvijek mora biti moguće. O tom okviru ovisi prikaz informacija o povezanim funkcijama i ostvarivanju prava. Kad korisnici žele ostvariti svoja prava, broj koraka trebao bi biti što manji. Korisnici bi trebali imati što izravniji pristup funkciji za ostvarivanje prava. Navigacija brojnim slojevima informacija prije stvarnog pristupa funkcijama za ostvarivanje prava mogla bi većinu korisnika odvratiti od ostvarivanja tih prava. Ako pružatelj usluga društvenih medija uvede velik broj koraka, trebao bi moći dokazati da to ide u prilog korisnicima kao ispitanicima na temelju OUZP-a. Osim što bi prava ispitanika trebala biti objašnjena u obavijesti o zaštiti privatnosti, kako je propisano člankom 13. stavkom 2. točkama (b), (c) i (d) OUZP-a, ostvarivanje prava trebalo bi biti dostupno i neovisno o tim informacijama. Na primjer, korisnici bi trebali moći ostvarivati prava ispitanika i preko izbornika platforme.

> **Primjer 17:** Pružatelj usluga društvenih medija na svojoj platformi objavljuje dokument pod nazivom „korisni savjeti", koji sadržava i važne informacije o ostvarivanju prava ispitanika. Međutim, pravila zaštite privatnosti ne sadržavaju nikakvu poveznicu ni drugo upućivanje na taj dokument. Umjesto toga, navodi se da je više pojedinosti dostupno u odjeljku s pitanjima i odgovorima na internetskim stranicama. Korisnici koji očekuju da će u pravilima zaštite privatnosti dobiti informacije o svojim pravima ondje neće pronaći ta objašnjenja i morat će pretraživati odjeljak s pitanjima i odgovorima.

82. Ovo je očigledan primjer obrasca ***labirint pravila privatnosti*** koji otežava pristup dodatnim informacijama o pravima ispitanika, a posebno o tome kako ih ostvariti, što je u suprotnosti s

[45] Vidjeti Smjernice o transparentnosti, primjer u točki 11.

[46] Za pojedinosti o slojevitom pristupu u digitalnom okruženju vidjeti Smjernice o transparentnosti, točke od 35. do 37.

člankom 12. stavkom 2. OUZP-a. Osim toga, ako su pravila zaštite privatnosti nepotpuna, time se krši i članak 13. stavak 2. točke (b), (c) i (d), kao i članak 14. stavak 2. točke (c), (d) i (e) OUZP-a. Naime, iako bi se detaljnijim informacijama ili izravnom načinu ostvarivanja prava moglo pristupiti jednim klikom s mjesta na kojem se spominju u pravilima zaštite privatnosti, korisnici u primjeru morat će otvoriti pitanja i odgovore te ih pretraživati kako bi pronašli dokument s korisnim savjetima.

83. Važno je napomenuti da su mogući čak i jači učinci od onih koje uzrokuje previše slojeva[47] ako se ne koristi samo više uređaja, nego i više aplikacija iste platforme društvenih medija, kao što su posebne aplikacije za razmjenu poruka. Korisnici takve sekundarne aplikacije naišli bi na veće prepreke i morali bi uložiti više truda ako bi morali otvoriti verziju u pregledniku ili primarnu aplikaciju kako bi dobili informacije povezane sa zaštitom podataka. U takvoj situaciji, kad se ne koristi samo više uređaja nego i više aplikacija, relevantne informacije uvijek moraju biti izravno dostupne neovisno o tome kako se korisnici služe platformom.

Ometanje – slijepa ulica (Prilog I., kontrolni popis 4.4.1.)

84. Do kršenja pravnih zahtjeva može doći i kad se informacije o zaštiti podataka propisane OUZP-om stave na raspolaganje daljnjim radnjama, kao što je klik na poveznicu ili gumb. Konkretno, pogrešna navigacija ili nedosljedan dizajn sučelja koji dovodi do neučinkovitih značajki ne može se smatrati poštenim u skladu s člankom 5. stavkom 1. točkom (a) OUZP-a jer se korisnike dovodi u zabludu ako pokušaju doći do informacija ili prilagoditi svoje preferencije zaštite podataka. ***Slijepe ulice*** u kojima su korisnici prepušteni sami sebi bez funkcija za ostvarivanje svojih prava u svakom bi slučaju trebalo izbjegavati i one dovode do izravne povrede članka 12. stavka 2. OUZP-a, u kojem je navedeno da voditelj obrade mora olakšati ostvarivanje prava.

Primjer 18: Pružatelj usluga društvenih medija u svojim pravilima zaštite privatnosti nudi brojne hiperveze na stranice s dodatnim informacijama o određenim temama. Međutim, više dijelova pravila zaštite privatnosti sadržava samo opće izjave da je moguće pristupiti dodatnim informacijama, ali nije navedeno gdje ni kako.

85. Pravila zaštite privatnosti općenito se smatraju dokumentom u kojem su centralizirane sve informacije o zaštiti podataka u skladu s obvezama utvrđenima u člancima 12., 13. i 14. OUZP-a. Stoga je potrebno omogućiti i preusmjeravanje na sva relevantna mjesta na platformi društvenih medija kako bi korisnici mogli nadzirati svoje podatke ili ostvariti svoja prava. U primjeru 18 to je samo djelomično postignuto jer su za neke elemente dostupne poveznice na dodatne informacije, dok za druge nisu. U tim slučajevima obrazac ***slijepa ulica*** može dovesti do povrede članka 12. stavka 1. OUZP-a jer otežava pristup nekim informacijama o zaštiti podataka ili članka 12. stavka 2. OUZP-a jer ne olakšava ostvarivanje prava.

d. **Primjeri dobre prakse**

Fiksna navigacija (eng. *sticky navigation*): za vrijeme pregledavanja stranice koja se odnosi na zaštitu podataka sadržaj se može stalno prikazivati na zaslonu, tako da se korisnici uvijek mogu snaći na stranici i brzo navigirati sadržajem zahvaljujući usidrenim poveznicama.

Povratak na vrh: postavite gumb za povratak na vrh na dno stranice ili kao fiksni element na dnu prozora da biste korisnicima olakšali navigaciju na stranici.

[47] Vidjeti točke 81. i 82.

Prečaci: vidjeti definiciju u scenariju uporabe 1 (str. 22). (*npr. u pravilima zaštite privatnosti za svaku informaciju o zaštiti podataka navedite poveznice koje izravno preusmjeravaju na povezane stranice o zaštiti podataka na platformi društvenih medija*).

Podaci za kontakt: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Obraćanje nadzornom tijelu: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Pregled pravila zaštite privatnosti: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Praćenje promjena i usporedba: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Usklađeni tekst: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Navođenje definicija: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Korištenje primjera: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Scenarij uporabe 2b: informiranje ispitanika o zajedničkom vođenju obrade, članak 26. stavak 2. OUZP-a

a. Opis konteksta i relevantne pravne odredbe

86. U drugoj rečenici članka 26. stavka 2. OUZP-a predviđene su dodatne odredbe o transparentnosti u posebnom slučaju zajedničkog vođenja obrade[48]. One osiguravaju da je bit dogovora o zajedničkom vođenju obrade dostupna ispitanicima[49]. U svojim Smjernicama 07/2020 o pojmovima voditelja i izvršitelja obrade u Općoj uredbi o zaštiti podataka EDPB preporučuje da ta bit obuhvati barem sve elemente informacija iz članaka 13. i 14. OUZP-a koji bi već trebali biti dostupni ispitanicima te da se za svaki od njih odredi koji je zajednički voditelj obrade odgovoran za postizanje usklađenosti s tim elementom[50]. Bit dogovora mora sadržavati i kontaktnu točku, ako je imenovana. Zajednički voditelji obrade trebaju odlučiti o najučinkovitijem načinu na koji će bit dogovora staviti na raspolaganje ispitanicima[51].

b. Obmanjujući obrasci dizajna

Primjer 19: Kad je riječ o obmanjujućim obrascima dizajna, voditelji obrade u toj konfiguraciji trebaju integrirati te informacije u internetski sustav tako da se mogu lako uočiti i ne gube na jasnoći i razumljivosti, iako se u članku 12. stavku 1. prvoj rečenici OUZP-a ne upućuje izravno na članak 26. stavak 2. drugu rečenicu OUZP-a. Međutim, zbog načela poštenosti, transparentnosti i pouzdanosti zaštite podataka iz članka 5. stavka 1. točke (a) i članka 5. stavka 2. OUZP-a usporedivi zahtjevi primjenjuju se i na pitanje zajedničkog vođenja obrade. Kad zajednički voditelji obrade u obavijesti o zaštiti privatnosti pružaju informacije o biti dogovora, i to trebaju učiniti jasno i transparentno. Zato se ne može ocijeniti da je obrada poštena ako je informacije o njoj teško razumjeti jer nisu navedene poveznice ili su

[48] Za definiciju zajedničkog vođenja obrade vidjeti članak 4. točku 7. u vezi s člankom 26. stavkom 1. prvom rečenicom OUZP-a te Smjernice 07/2020 EDPB-a o pojmovima voditelja obrade i izvršitelja obrade u Općoj uredbi o zaštiti podataka, donesene 7. srpnja 2021., verziju 2.1., točke od 46. do 49., dostupne na https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.
[49] Vidjeti Smjernice EDPB-a 07/2020 o voditelju obrade i izvršitelju obrade, točku 179.
[50] Vidjeti Smjernice EDPB-a 07/2020 o voditelju obrade i izvršitelju obrade, točku 180., vrijedi i za sljedeću rečenicu.
[51] Smjernice EDPB-a 07/2020 o voditelju obrade i izvršitelju obrade, točka 181.

informacije raspoređene u više područja. Obmanjujući obrazac dizajna poznat kao ***labirint pravila privatnosti***[52] mogao bi biti još više zbunjujući jer u obavijesti o zaštiti privatnosti korisnici općenito mogu očekivati da će se informacije iz članka 26. stavka 2. druge rečenice OUZP-a navesti u cjelovitom obliku. Pružatelj usluga društvenih medija u pravilima zaštite privatnosti uvijek spominje „podatke za izradu" i ne koristi pojam „osobni podaci". Samo slojevita obavijest o zaštiti privatnosti na stranici 90 sadržava objašnjenje da „podaci za izradu mogu uključivati osobne podatke korisnika". Pojam „podaci za izradu" spominje se bez objašnjenja i u biti dogovora o zajedničkim voditeljima obrade koja je dostupna ispitanicima. Drugi zajednički voditelj obrade (B) u svojim pravilima zaštite privatnosti navodi definiciju osobnih podataka. Međutim, u odjeljku o pravilima zaštite privatnosti koji se odnosi na zajedničko vođenje obrade podataka s pružateljem usluga društvenih medija B navodi samo poveznicu na ugovor koji je dostavio pružatelj usluga društvenih medija bez dodatnog objašnjenja.

87. Objašnjenja iz članka 26. stavka 2. druge rečenice OUZP-a teže je razumjeti ako više nisu dosljedna. Taj se učinak nedosljednosti pojačava kad platforme društvenih medija koriste vlastitu terminologiju koju korisnici obično ne povezuju s obradom osobnih podataka, kao što je prikazano u gornjem primjeru 19. U tom primjeru oba zajednička voditelja obrade krše članak 26. stavak 2. drugu rečenicu OUZP-a i članak 5. stavak 1. točku (a) OUZP-a jer su informacije o zajedničkom vođenju obrade nejasne, a time i netransparentne za ispitanike.

Scenarij uporabe 2c: obavješćivanje ispitanika o povredi osobnih podataka

a. Opis konteksta i relevantne pravne odredbe

88. Kako bi voditelj obrade mogao utvrditi i odgovoriti na povredu podataka, prvo je mora prepoznati[53]. U skladu s člankom 4. točkom 12. OUZP-a „povreda osobnih podataka" znači „kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani". Kad je riječ o voditeljima obrade na društvenim medijima, povrede podataka mogu se dogoditi na više načina. Na primjer, napadač može pristupiti osobnim podacima i porukama korisnika na usluzi razgovora. Alternativna je mogućnost da zbog pogreške u programiranju aplikacija pristupi osobnim podacima izvan opsega dopuštenja koja su dali korisnici. Drugi bi primjer bio da korisnici podijele fotografije uz postavku „dijeljenje s najboljim prijateljima", ali te slike postanu vidljive širem krugu ljudi. Naposljetku, platforma društvenih medija koja se temelji na dijeljenju videozapisa u stvarnom vremenu zbog greške bi mogla nastaviti dijeliti prijenos sadržaja unatoč tome što su korisnici prethodno pritisnuli gumb za zaustavljanje snimanja.

89. U slučaju povrede osobnih podataka voditelj obrade dužan je u svakom slučaju obavijestiti nadležno nadzorno tijelo u skladu s člankom 33. OUZP-a, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako je vjerojatno da će povreda podataka prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade dužan je općenito o takvoj povredi obavijestiti i ispitanike u skladu s člankom 34. stavcima 1. i 2. OUZP-a. U tom slučaju voditelj obrade

[52] Vidjeti scenarij uporabe 2a, primjer 17 u ovim Smjernicama.

[53] Vidjeti i Smjernice EDPB-a 01/2021 o primjerima obavješćivanja o povredi osobnih podataka, donesene 14. prosinca 2021., verziju 2.0, točku 4., dostupne na https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_hr.pdf.

mora obavijestiti ispitanike bez nepotrebnog odgađanja. Obavijest mora sadržavati opis prirode povrede osobnih podataka pisan jasnim i jednostavnim jezikom jer se primjenjuje i članak 12. OUZP-a. Nadalje, te informacije moraju sadržavati barem informacije i mjere kao što su (vidjeti i članak 33. stavak 3. točke od (b) do (d) u vezi s člankom 34. stavkom 2. OUZP-a):

- ime i kontaktni podaci službenika za zaštitu podataka, ako postoji, ili druge kontaktne točke od koje se može dobiti još informacija
- opis vjerojatnih posljedica povrede osobnih podataka i
- opis mjera koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica[54].

90. Takve obavijesti o povredi podataka u skladu s člankom 34. OUZP-a isto tako mogu sadržavati obmanjujuće obrasce dizajna. Na primjer, ako odgovarajući voditelj obrade ispitanicima pruži sve potrebne informacije kako bi ih obavijestio o opsegu povrede podataka, ali im pruži i neodređene i nerelevantne informacije o njezinim posljedicama i mjerama predostrožnosti koje je voditelj obrade poduzeo ili predložio poduzeti. Te djelomično nerelevantne informacije mogu zavarati, a korisnici pogođeni povredom možda neće u potpunosti razumjeti posljedice povrede ili će podcijeniti njezine (potencijalne) učinke.

b. Obmanjujući obrasci dizajna

91. U nastavku se navodi nekoliko negativnih primjera zlouporabe obavijesti o povredi podataka kojima se krši članak 34. OUZP-a u vezi s člankom 12. OUZP-a:

i. Obrasci koji se temelje na sadržaju

Držanje u neznanju – proturječne informacije (Prilog I., kontrolni popis 4.6.2.)

Primjer 20:

- Voditelj obrade upućuje samo na radnje treće strane i navodi da je povredu podataka uzrokovala treća strana (npr. izvršitelj obrade) te da stoga nije došlo do povrede sigurnosti. Voditelj obrade ističe i neke primjere dobre prakse koji nisu povezani sa stvarnom povredom.
- Voditelj obrade utvrđuje ozbiljnost povrede iz svoje perspektive ili perspektive izvršitelja obrade umjesto da se usredotoči na ispitanika.

Držanje u neznanju – dvosmisleni tekst ili informacije (Prilog I., kontrolni popis 4.6.3.)

92. Pri obavješćivanju ispitanika o povredi voditelji obrade svakako moraju imati na umu da većina primatelja nije naviknuta na specifičan tehnički ili pravni jezik povezan sa zaštitom podataka.

Primjer 21: Zbog povrede podataka na platformi društvenih medija neovlaštenim korisnicima slučajno je objavljeno više skupova zdravstvenih podataka. Pružatelj usluga društvenih medija obavještava korisnike samo da su „posebne kategorije osobnih podataka" slučajno postale javne.

[54] Smjernice Radne skupine iz članka 29. o obavješćivanju o povredi osobnih podataka, koje je odobrio EDPB, str. 20. https://ec.europa.eu/newsroom/article29/items/612052/hr.

93. Riječ je o ***dvosmislenom tekstu*** jer prosječni korisnici ne razumiju pojam „posebne kategorije osobnih podataka" i zato ne znaju da su objavljeni njihovi zdravstveni podaci. To se može objasniti činjenicom da pojam „poseban" u općem jeziku ima znatno drukčije značenje u odnosu na specifičan jezik OUZP-a. Prosječni korisnici ne znaju da se u skladu s člankom 9. stavkom 1. OUZP-a „posebne kategorije osobnih podataka" odnose na osobne podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te podatke obuhvaćene obradom genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca ili podatke koji se odnose na zdravlje ili podatke o spolnom životu ili seksualnoj orijentaciji pojedinca. Prema tome, izraz „posebne kategorije osobnih podataka" u ovom je scenariju obmanjujući uzorak dizajna jer ne sadržava dodatna objašnjenja i tako zavarava korisnike. To je primjer situacije u kojoj voditelj obrade pokušava obavijestiti ispitanike o povredi, ali ne ispunjava u potpunosti svoju obvezu obavješćivanja o povredi podataka u skladu s člankom 34. OUZP-a jer će prosječni čitatelj podcijeniti ozbiljnost incidenta. Osim toga, kratke informacije u primjeru nisu razumljive kako je propisano člankom 34. u vezi s člankom 12. stavkom 1. prvom rečenicom OUZP-a.

94. U nastavku se navodi još jedan primjer ***dvosmislenog teksta***:

Primjer 22: Pri nabrajanju pogođenih kategorija osobnih podataka voditelj obrade spominje samo nejasne pojedinosti; na primjer, upućuje na dokumente koje su dostavili korisnici, ali ne navodi koje kategorije osobnih podataka ti dokumenti sadržavaju i koliko su osjetljivi.

95. Važno je napomenuti da se taj obmanjujući obrazac dizajna može pojaviti u svim dijelovima obavijesti o povredi podataka. Dok se dva navedena primjera odnose na nejasno formuliran tekst o pogođenim kategorijama podataka, sljedeći primjer pokazuje da bi i kategorija pogođenih ispitanika mogla biti jednako nejasna:

Primjer 23: Pri izvješćivanju o povredi voditelj obrade ne navodi dovoljno precizno kategoriju pogođenih ispitanika; na primjer, spominje samo da je riječ o učenicima, ali ne navodi jesu li maloljetni odnosno pripadaju li skupinama ranjivih ispitanika.

96. Naposljetku, zbog pružanja ***dvosmislenih informacija*** može se podcijeniti ozbiljnost incidenta kao u sljedećem primjeru:

Primjer 24: Pri obavješćivanju nadzornog tijela i ispitanika o povredi voditelj obrade izjavljuje da su osobni podaci objavljeni iz drugih izvora. Zbog toga ispitanik smatra da nije došlo do povrede sigurnosti.

ii. Obrasci koji se temelje na sučelju

97. Kao što je opisano u nastavku, negativni primjeri obavijesti o povredi podataka mogu biti i obmanjujući obrasci dizajna koji se temelje na sučelju suprotno članku 34. OUZP-a u vezi s člankom 12. OUZP-a:

Preskakanje – odvraćanje pozornosti (Prilog I., kontrolni popis 4.2.2.)

Primjer 25:

• U tekstovima izvješća voditelja obrade navedene su brojne nevažne informacije, a izostavljene su važne pojedinosti.

- Ako su povredom sigurnosti obuhvaćene vjerodajnice za pristup i druge vrste podataka, voditelj obrade izjavljuje da su podaci zaštićeni enkripcijom ili raspršeni (eng. *hashing*), iako to vrijedi samo za lozinke.

98. U tom slučaju, čak i ako izvješće sadržava relevantne pojedinosti, ispitanici će ih vjerojatno previdjeti jer su preopterećeni nevažnim informacijama.

c. Primjeri dobre prakse

Obavijesti: obavijesti mogu korisnike informirati o aspektima, promjenama ili rizicima povezanima s obradom osobnih podataka (*npr. kad je došlo do povrede podataka*). Te obavijesti mogu se dostavljati u više oblika, kao što su poruke u ulaznom spremniku računa, skočni prozori ili fiksne obavijesti na vrhu internetske stranice.

Objašnjavanje posljedica: ako korisnici žele aktivirati ili deaktivirati kontrolu zaštite podataka ili dati ili povući privolu, obavijestite ih o posljedicama te radnje neutralnim tonom.

Prečaci: vidjeti definiciju u scenariju uporabe 1 (str. 22) (*npr. korisnicima osigurajte poveznicu za ponovno postavljanje lozinke*).

Usklađeni tekst: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Navođenje definicija: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Korištenje primjera: vidjeti definiciju u scenariju uporabe 1 (str. 22).

3.3. Zaštita na društvenim medijima

Scenarij uporabe 3a: upravljanje privolom za vrijeme korištenja platforme društvenih medija

a. Opis konteksta i relevantne pravne odredbe

99. Korisnici platformi društvenih medija moraju dati privolu u raznim fazama obrade podataka, na primjer za primanje personaliziranih oglasa. Kako je već navedeno u Smjernicama EDPB-a o ciljanju korisnika društvenih medija, privola može biti odgovarajuća pravna osnova samo ako se ispitaniku omoguće kontrola i stvaran izbor55. Osim toga, u skladu s člankom 4. točkom 11. OUZP-a privola mora biti posebna, informirana i nedvosmislena56. Važno je naglasiti da zahtjevi za valjanu privolu u skladu s OUZP-om nisu dodatna obveza, već preduvjeti za zakonitu obradu osobnih podataka korisnika. Nadalje, na internetski marketing i metode internetskog praćenja primjenjuje se Direktiva 2002/58/EZ (Direktiva o e-privatnosti). Međutim, preduvjeti za valjanu privolu u skladu s Direktivom o e-privatnosti jednaki su odredbama povezanima s privolom iz OUZP-a57.

100. S obzirom na načelo pouzdanosti iz članka 5. stavka 2. OUZP-a i potrebu da voditelj obrade može dokazati da su ispitanici dali privolu za obradu svojih osobnih podataka u skladu s člankom 7. stavkom 1. OUZP-a neophodno je da pružatelj usluga društvenih medija može dokazati da je pravilno prikupio privolu korisnika. Može biti teško dokazati da je taj uvjet ispunjen, na primjer ako korisnici trebaju dati privolu prihvaćanjem kolačića. Nadalje, ispitanici katkad možda ne znaju da daju privolu

[55] Smjernice 8/2020 o ciljanju korisnika društvenih medija, točka 51.
[56] Vidjeti i točke od 25. do 29.
[57] Vidjeti članak 2. točku (f) Direktive 2002/58/EZ i Mišljenje EDPB-a 5/2019 o povezanosti Direktive o e-privatnosti i Opće uredbe o zaštiti podataka, posebice u vezi s nadležnosti, zadaćama i ovlastima tijela za zaštitu podataka, doneseno 12. ožujka 2019., točku 14. https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_hr.

ako brzo kliknu na istaknuti gumb ili unaprijed postavljene opcije. Unatoč tome, kako je istaknuto u članku 7. stavku 1. OUZP-a, teret dokazivanja da su korisnici dobrovoljno dali privolu snosi voditelj obrade.

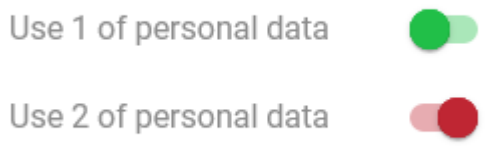
b. Obmanjujući obrasci dizajna

i. Obrasci koji se temelje na sadržaju

101. Osim već objašnjenih obrazaca koji se temelje na sadržaju, a koji bi se mogli primjenjivati na informacije povezane sa zahtjevom za privolu[58], u kontekstu privole moguća su još dva obmanjujuća obrasca dizajna koja se temelje na sadržaju.

Proturječne informacije – držanje u neznanju (Prilog I., kontrolni popis 4.6.2.)

Primjer 26: Sučelje sadržava preklopni gumb kojim korisnici mogu dati ili povući privolu. Međutim, iz dizajna preklopnog gumba nije jasno u kojem je položaju i jesu li korisnici dali privolu ili ne. Naime, položaj gumba ne odgovara boji. Ako je preklopni gumb na desnoj strani, što se obično povezuje s aktivacijom značajke („uključivanje"), poprima crvenu boju, koja obično upućuje na to da je značajka isključena. S druge strane, kad je gumb na lijevoj strani, što obično znači da je značajka isključena, pozadina gumba je zelene boje, koja se obično povezuje s aktivnom opcijom.



102. Ako se pri prikupljanju privole daju ***proturječne informacije***, te su informacije nejasne i nerazumljive. U gornjem primjeru prikazan je slučaj u kojem su vizualne informacije nejasne. Korisnici koji naiđu na takve gumbe neće biti sigurni jesu li dali privolu. Ako su vizualne oznake tako pomiješane ili prikazane drugim bojama koje se čine proturječnima stvarnom okruženju, kao u primjeru 26, u kojem je prikazan samo jedan slučaj zbunjujućih preklopnih gumba, ne može se smatrati da je privola dana nedvosmisleno u skladu s člankom 7. stavkom 2. OUZP-a u vezi s člankom 4. točkom 11. OUZP-a. ***Proturječne informacije*** mogu se dati i tekstom, kako je prikazano u nastavku.

Primjer 27: Pružatelj usluga društvenih medija korisnicima daje proturječne informacije: iako se u informacijama prvo navodi da se kontakti ne uvoze bez privole, u skočnom prozoru istodobno se objašnjava da će se kontakti ipak uvoziti.

Ometanje – zavaravajuća radnja (Prilog I., kontrolni popis 4.4.3.)

103. Osim ***proturječnih informacija*** voditelji obrade mogu pružati informacije koje zavaravaju korisnike jer ne odgovaraju njihovim očekivanjima. ***Zavaravajuća radnja*** je slučaj kad nepodudarnost između

[58] Vidjeti scenarij uporabe 1, točke od 32. do 49. ili primjere iz scenarija uporabe 1 navedene u Prilogu.

informacija i raspoloživih radnji potakne korisnike da učine nešto što ne namjeravaju. Budući da je ono što korisnici dobiju različito od onog što očekuju, vjerojatno će odustati od daljnjih koraka.

Primjer 28: Korisnik pregledava objave na društvenim medijima. Pritom mu se prikazuju oglasi. Zaintrigiran jednim oglasom i u želji da dozna zašto mu se prikazuje korisnik klikne na znak „?" u donjem desnom kutu oglasa. Otvara se skočni prozor u kojem je objašnjeno zašto korisnik vidi taj oglas te su navedeni kriteriji ciljanja. Korisnik se ujedno obavještava da može povući privolu za ciljano oglašavanje te mu se nudi poveznica za tu radnju. Kad korisnik klikne na tu poveznicu, preusmjerava se na sasvim druge internetske stranice koje sadržavaju opća objašnjenja o tome što je privola i kako njome upravljati.

104. Navedeni slučaj primjer je sadržaja koji ne odgovara očekivanjima korisnika. Naime, kad korisnici kliknu na poveznicu, očekuju da će biti preusmjereni na stranicu na kojoj će moći izravno povući privolu. Umjesto toga otvara se stranica na kojoj to ne mogu učiniti i ne navodi se konkretan način povlačenja privole na predmetnoj platformi društvenih medija. Taj raskorak između onoga što bi trebali pronaći i onoga što zapravo pronađu vjerojatno će zbuniti korisnike, koji neće biti sigurni kako postupiti. U najgorem slučaju mogli bi pretpostaviti da ne mogu povući privolu. Takva ***zavaravajuća radnja*** ne može se smatrati transparentnim kako je propisano člankom 12. stavkom 1. OUZP-a. Osim toga, tom bi se praksom mogao prekršiti članak 7. stavak 3. OUZP-a ako se pri usporedbi postupaka povlačenja i prikupljanja privole pokaže da je povlačenje privole teže od njezina davanja.

105. Ako pružatelji usluga društvenih medija obavijeste korisnike da njihova radnja može imati određenu posljedicu, a ta radnja zapravo dovodi do drukčijeg ishoda, riječ je o ***zavaravajućoj radnji***, kao što je prikazano u sljedećem primjeru.

Primjer 29: U odjeljku računa na društvenim medijima predviđenom za dijeljenje misli, fotografija itd. od korisnika se traži da potvrdi da želi podijeliti taj sadržaj nakon što ga unesu ili prenesu. Korisnik može birati između gumba na kojem piše „Da, svakako." i drugog na kojem piše „Ne, hvala." Međutim, nakon što korisnik odluči da ne želi dijeliti sadržaj s drugim korisnicima i klikne na drugi gumb, sadržaj se objavljuje na njegovu računu na društvenim medijima.

106. Kao i u prethodnom primjeru, navedene informacije nisu transparentne i korisnicima oduzimaju mogućnost izbora. Iako korisnik može brzo primijetiti objavu i izbrisati je, podaci su obrađeni i objavljeni drugim korisnicima unatoč njegovu odbijanju. Još je sporniji primjer kad obrada nije uočljiva korisnicima ili je uočljiva samo uz poteškoće ili poznavanje informacijske tehnologije jer se odvija u pozadini platforme društvenih medija.

ii. Obrasci koji se temelje na sučelju

107. Osim navedenih dvaju obmanjujućih uzoraka dizajna, u ovom su scenariju uporabe relevantni uglavnom uzorci koji se temelje na sučelju.

Preskakanje – odvraćanje pozornosti (Prilog I., kontrolni popis 4.2.2.)

108. Ako se radnja ili informacije povezane sa zaštitom podataka nude istodobno s drugim elementom koji može, ali i ne mora biti povezan sa zaštitom podataka, i ako korisnici odaberu tu drugu opciju,

vjerojatno će zaboraviti na element zaštite podataka, čak i ako su prvotno bili usredotočeni na njega. Riječ je o obrascu poznatom kao **odvraćanje pozornosti**, koji se procjenjuje na pojedinačnoj osnovi.

> **Primjer 30:** U obavijesti o kolačićima na platformi društvenih medija piše: „Za slasne kolačiće potrebni su vam samo maslac, šećer i brašno. Pogledajte naš omiljeni recept ovdje [poveznica]. I mi koristimo kolačiće. Pročitajte više u našim pravilima o kolačićima [poveznica].” te je prikazan gumb za potvrdu.

109. Humor se ne smije iskorištavati za pogrešno prikazivanje potencijalnih rizika i umanjivanje pouzdanosti stvarnih informacija. U ovom primjeru korisnici bi mogli doći u iskušenje da kliknu samo na prvu poveznicu, pročitaju recept za kolačiće i zatim kliknu na gumb za potvrdu. U ovom primjeru opisan je slučaj u kojem, osim što korisnicima nije omogućeno da daju privolu, privola možda nije dovoljno informirana. Naime, korisnici bi mogli misliti da klikom na gumb za potvrdu samo odbacuju smiješnu poruku o kolačićima kao poslastici i zanemariti tehničko značenje pojma „kolačići”. Taj slučaj ne bi se smatrao informiranom privolom u smislu članka 7. stavka 2. OUZP-a u vezi s člankom 4. točkom 11. OUZP-a.

110. U članku 7. stavku 2. OUZP-a nadalje se navodi da bi se zahtjev za privolu trebao moći jasno razlučiti od drugih pitanja. Stoga je bitno da informacije o zaštiti podataka ne zasjeni drugi kontekst. Zbog igre riječi s homonimima „kolačić” u ovom primjeru kontekst slastica mogao bi zasjeniti kontekst zaštite podataka. Da bi se zadovoljio kriterij jasne razlučivosti, informacije koje su korisnicima relevantne za davanje valjane privole trebale bi biti istaknute, a ne ***skrivene na vidljivom mjestu*** ni pomiješane s drugim pitanjima ili značenjima. Ne bi trebalo biti zabune između informacija o zaštiti podataka i drugih vrsta sadržaja. U suprotnom bi se korisnicima mogla odvratiti pozornost od stvarnih posljedica obrade njihovih osobnih podataka. Pri provedbi tih preduvjeta dizajnerima treba omogućiti određenu kreativnu slobodu kako bi informacije zvučale privlačno.

Ometanje – slijepa ulica (Prilog I., kontrolni popis 4.4.1.)

111. Zbunjivanje ili odvraćanje pozornosti nisu jedini mogući učinci obmanjujućih obrazaca dizajna povezani s privolom. Točnije, obrazac ***slijepa ulica*** može na više načina utjecati na uvjete privole iz članka 7. OUZP-a u vezi s člankom 4. točkom 11. OUZP-a.

> **Primjer 31:** Korisnik želi upravljati dopuštenjima koja je dao platformi društvenih medija na temelju privole. U postavkama mora pronaći stranicu povezanu s tim konkretnim radnjama jer želi onemogućiti dijeljenje svojih osobnih podataka u svrhe istraživanja. Kad korisnik klikne na polje kako bi uklonio oznaku, na razini sučelja ništa se ne događa i on stječe dojam da se privola ne može povući.

112. U ovom konkretnom primjeru obrazac ***slijepa ulica*** mogao bi prekršiti članak 7. stavak 3. OUZP-a jer se čini da korisnik ne može povući privolu za obradu svojih osobnih podataka u svrhe istraživanja jer za to predviđena značajka ne funkcionira. Ako radnja korisnika nije pravilno registrirana u sustavu, može doći do povrede članka 7. stavka 3. OUZP-a. Ako je izbor zapravo registriran u sustavu, moglo bi se smatrati da se time što radnja korisnika nije vidljiva na sučelju krši načelo poštenosti iz članka 5. stavka 1. točke (a) OUZP-a. Ako se čini da korisnici na sučelju mogu pravilno upravljati privolom, odnosno dati je ili povući, ali interakcija s njim ne proizvodi nikakav vizualan učinak, riječ je o zavaravanju korisnika, koji se osjeća zbunjeno, pa čak i frustrirano. Trebalo bi izbjegavati taj raskorak između stanja sustava i informacija koje prenosi sučelje jer korisnicima općenito može otežati nadzor njihovih osobnih podataka.

113. Brojne aktivnosti obrade uključuju više strana, odnosno osim voditelja obrade ili izvršitelja obrade s kojim je ispitanik u izravnom kontaktu u njima sudjeluje još jedan (zajednički) voditelj obrade ili još jedan izvršitelj obrade.

> **Primjer 32:** Pri obradi osobnih podataka svojih korisnika pružatelj usluga društvenih medija surađuje s trećim stranama. U svojim pravilima zaštite privatnosti navodi popis tih trećih strana u kojem nema poveznica na njihova pravila zaštite privatnosti, nego se samo upućuje korisnike da posjete njihove internetske stranice kako bi dobili informacije o tome kako ti subjekti obrađuju podatke i ostvarili svoja prava.

114. Taj primjer obrasca ***slijepa ulica*** pokazuje kako se korisnicima otežava pristup informacijama o predmetnoj obradi. Budući da vjerojatno neće dobiti sve relevantne informacije o obradi, moglo bi se smatrati da se takvom praksom krše zahtjevi lako dostupnih informacija iz članka 12. stavka 1. OUZP-a. Primjenom takve prakse na informacije koje se pružaju radi prikupljanja privole mogu se prekršiti zahtjevi za informiranu privolu navedeni u članku 7. stavku 2. u vezi s člankom 4. točkom 11. OUZP-a jer bi pristup informacijama bio previše otežan, pa ispitanici ne bi bili potpuno upoznati s posljedicama svojeg izbora.

Ometanje – dulje trajanje od nužnog (Prilog I., kontrolni popis 4.4.2.)

115. U članku 7. stavku 3. OUZP-a navodi se da bi povlačenje privole trebalo biti jednako jednostavno kao i njezino davanje. U Smjernicama 5/2020 o privoli na temelju Uredbe 2016/679 to se pitanje dodatno razrađuje te se navodi da bi trebalo omogućiti davanje i povlačenje privole istom radnjom. To podrazumijeva korištenje istog sučelja, ali i da mehanizmi za povlačenje privole trebaju biti lako dostupni, na primjer u obliku poveznice ili ikone koja je uvijek dostupna pri korištenju platforme društvenih medija.

> **Primjer 33:** Pružatelj usluga društvenih medija ne omogućuje izravno isključivanje obrade radi prikazivanja ciljanih oglasa, iako je za privolu (prihvaćanje) potreban samo jedan klik.

116. Stvarna jednostavnost povlačenja privole može se procijeniti mjerenjem vremena ili broja klikova potrebnih za obavljanje te radnje. Primjenom obmanjujućeg obrasca dizajna poznatog kao***dulje trajanje od nužnog*** u postupku povlačenja privole korisnika, kao što je prikazano u primjeru 33, u suprotnosti je s tim načelima i dovodi do povrede članka 7. stavka 3. OUZP-a.

Preopterećenost – labirint pravila privatnosti (Prilog I., kontrolni popis 4.1.2.)

117. Kako je istaknuto u Smjernicama 5/2020 o privoli, ispitanicima se moraju pružiti informacije o obradi na temelju privole kako bi mogli donijeti utemeljenu odluku[59]. Bez toga privola se ne može smatrati valjanom. U istim smjernicama dodatno se razrađuje kako pružati informacije i kao mogući primjer navodi se slojeviti pristup. Međutim, kao što je opisano u scenariju uporabe 2a[60], pri slojevitom pružanju informacija o zahtjevu za privolu pružatelji usluga društvenih medija moraju izbjegavati obmanjujući obrazac dizajna ***labirint pravila privatnosti***. Ako pronalaženje određenih informacija postane prezahtjevno jer bi ispitanici morali pregledavati više stranica ili dokumenata, privola dobivena pružanjem takvih informacija ne može se smatrati informiranom, što je protivno članku 7. OUZP-a u

[59] Smjernice 5/2020 o privoli, točke od 62. do 64.
[60] Vidjeti točke od 79. do 81.

vezi s člankom 4. točkom 11. OUZP-a. To bi ujedno značilo i da privola nije valjana i da je pružatelj usluga društvenih medija prekršio članak 6. OUZP-a.

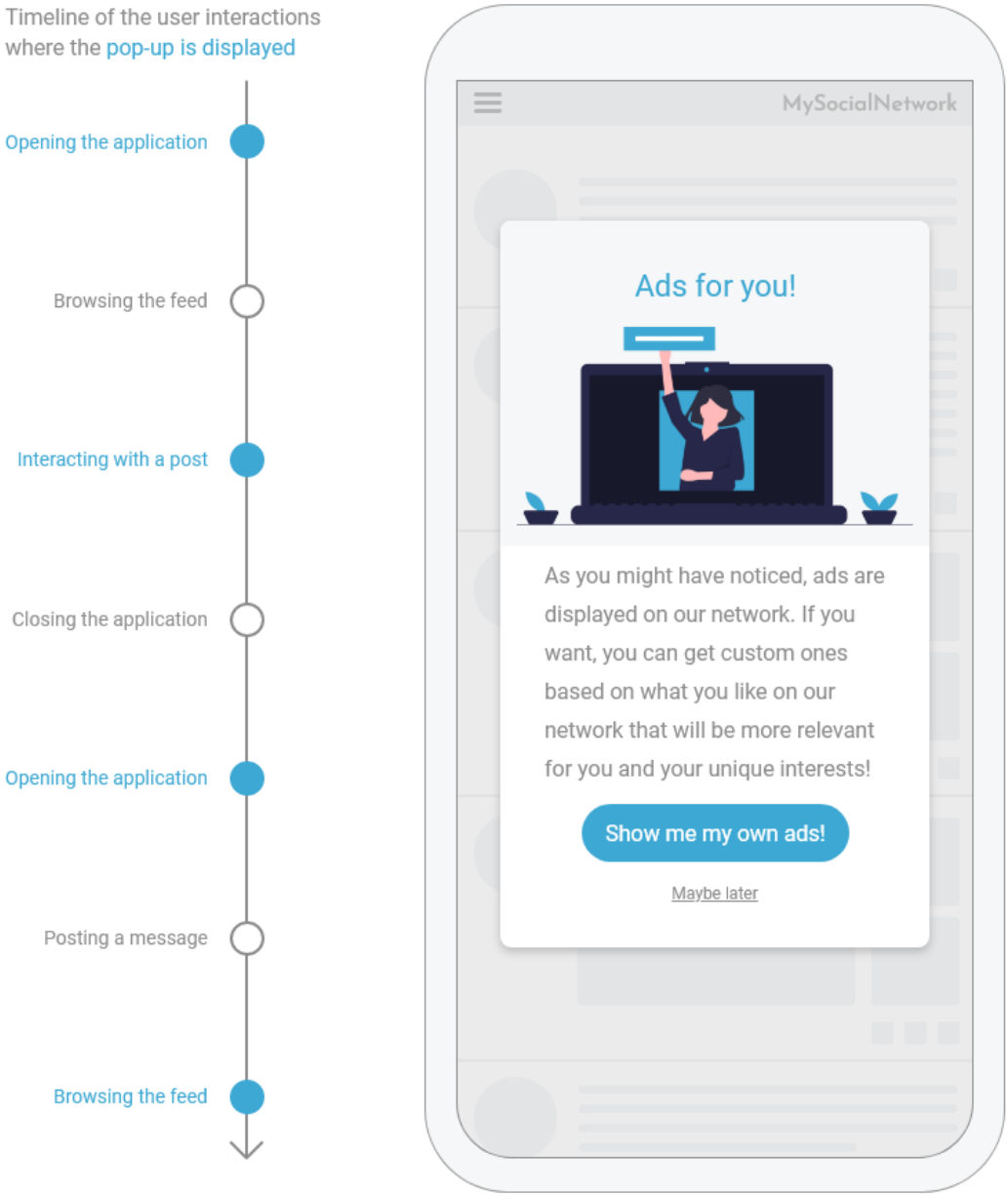
Primjer 34: Informacije za povlačenje privole dostupne su klikom na poveznicu kojoj se može pristupiti samo pregledavanjem svakog dijela računa i informacija povezanih s oglasima koji se prikazuju pri pregledavanju objava na društvenim medijima.

118. Kao što je opisano u gornjem scenariju, obmanjujući obrazac dizajna ***labirint pravila privatnosti*** može se pojaviti i nakon dobivanja privole ako se ne poštuje uvjet iz članka 7. stavka 3. četvrte rečenice OUZP-a, u kojem se navodi da povlačenje privole mora biti jednako jednostavno kao i njezino davanje. Problem je u tome što povlačenje privole uključuje više koraka nego njezino davanje. Budući da navedene informacije ujedno nisu lako dostupne ispitaniku jer su raspoređene po različitim dijelovima stranice, krši se načelo iz članka 12. stavka 1. OUZP-a.

Preopterećenost – kontinuirano prikazivanje upita (Prilog I., kontrolni popis 4.1.1.)

119. ***Kontinuirano prikazivanje upita*** korisnicima koji nisu dali privolu za obradu njihovih osobnih podataka u određenu svrhu ometa ih u redovnom korištenju društvenih medija. To znači da korisnici ne mogu uskratiti, a stoga ni povući privolu bez štetnih posljedica. To je protivno uvjetu dobrovoljne privole u skladu s člankom 7. u vezi s člankom 4. točkom 11. OUZP-a, prema kojem privola znači svako dobrovoljno izražavanje želja ispitanika kojim oni daju pristanak na obradu osobnih podataka koji se na njih odnose. U uvodnoj izjavi 42. petoj rečenici OUZP-a nadalje se navodi da se ne može smatrati da je privola dana dobrovoljno ako ispitanik nema istinski ili slobodan izbor. To potvrđuju i Smjernice EDPB-a o privoli, u kojima se navodi da privola neće biti valjana ako ispitanici nemaju istinski izbor ili smatraju da su obvezni pristati zbog bilo kojeg oblika neprimjerenog pritiska ili utjecaja na njih koji ih sprečava da ostvare svoju slobodnu volju[61]. Budući da ***kontinuirano prikazivanje upita*** može stvoriti takvu vrstu pritiska, njime se krši načelo dobrovoljne privole. Osim toga, budući da nije vjerojatno da će pružatelj usluga društvenih medija nakon što korisnici daju privolu redovito (npr. svaki put kad se korisnik prijavi na svoj račun) nuditi mogućnost povlačenja privole, taj obmanjujući obrazac dizajna može se kršiti članak 7. stavak 3. četvrta rečenica OUZP-a, u kojem se navodi da povlačenje privole mora biti jednako jednostavno kao i njezino davanje („učinak zrcala”).

[61] Smjernice 5/2020 o privoli, točke od 13. do 14.



Primjer 35: U ovom primjeru korisnike se pri izradi računa pita prihvaćaju li obradu njihovih podataka kako bi im se prikazivali personalizirani oglasi. Ako korisnici tijekom registracije uskrate privolu za tu uporabu podataka, pri korištenju društvene mreže redovito im se pojavljuje prethodno ilustrirani okvir s pitanjem žele li da im se prikazuju personalizirani oglasi. Taj okvir onemogućuje im korištenje društvene mreže. Budući da se prikazuje redovito, to ***kontinuirano prikazivanje upita*** iscrpit će korisnike, zbog čega će vjerojatno dati privolu za personalizirano oglašavanje. Nadalje, na ovom sučelju koristi se i obrazac ***skrivanje na vidljivom mjestu***[62] jer je radnja za prihvaćanje oglasa znatno uočljivija od opcije odbijanja.

120. Osim toga, voditelj obrade mogao bi prekršiti načelo poštenosti u smislu članka 5. stavka 1. točke (a) OUZP-a. Budući da korisnici u navedenom primjeru pri izradi svojeg računa nisu jasnom radnjom dali privolu za obradu njihovih osobnih podataka radi prikazivanja ciljanih oglasa, opterećuje ih ponavljanje

[62] Vidjeti točku 49. ili dio 4.3.2. Priloga.

upita koji stalno dovode u pitanje jasno odbijanje koje su izrazili. Ta jasna radnja koju su korisnici poduzeli u postupku registracije sada se stalno propituje. Time se korisničko iskustvo znatno pogoršava, što povećava vjerojatnost da će korisnici u jednom trenutku prihvatiti prikazivanje ciljanih oglasa samo kako bi izbjegli da im se upit ponovno prikazuje pri svakoj prijavi u račun radi korištenja platforme društvenih medija. U ovom slučaju uskraćivanje privole izravno utječe na kvalitetu usluge koja se pruža korisnicima i uvjetuje izvršenje ugovora.

c. Primjeri dobre prakse

Dosljednost na različitim uređajima: ako je platforma društvenih medija dostupna na različitim uređajima (npr. računalo, pametni telefoni), postavke i informacije povezane sa zaštitom podataka trebale bi se nalaziti na istim mjestima u različitim verzijama i obuhvaćati iste korake i elemente sučelja (izbornik, ikone itd.).

Praćenje promjena i usporedba: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Usklađeni tekst: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Navođenje definicija: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Korištenje primjera: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Fiksna navigacija (eng. *sticky navigation*): vidjeti definiciju u scenariju uporabe 2a (str. 28).

Povratak na vrh: vidjeti definiciju u scenariju uporabe 2a (str. 28).

Obavijesti: vidjeti definiciju u scenariju uporabe 2c (str. 32).

Objašnjavanje posljedica: vidjeti definiciju u scenariju uporabe 2c (str. 32).

Scenarij uporabe 3b: upravljanje postavkama zaštite podataka

a. Opis konteksta

121. Nakon postupka registracije i za vrijeme cijelog životnog ciklusa računa na društvenim medijima korisnici bi trebali moći prilagoditi svoje postavke zaštite podataka.

122. Bez obzira na to jesu li korisnici otprije upoznati sa zaštitom podataka općenito i konkretno s OUZP-om te vode li računa o tome koje osobne podatke žele ili ne žele dijeliti i objavljivati drugim korisnicima, svi imaju pravo na transparentne informacije o svojim mogućnostima dok koriste društvene medije.

123. Korisnici na platformama društvenih medija dijele veliku količinu osobnih podataka. Platforme društvenih medija često ih potiču da redovito dijele više sadržaja. Iako korisnici možda žele podijeliti trenutke svojeg života, sudjelovati u raspravi o određenoj temi ili proširiti mrežu kontakata iz profesionalnih ili osobnih razloga, mora im se omogućiti da nadziru tko može vidjeti koje dijelove njihovih osobnih podataka. Umnožavanje broja koraka potrebnih za promjenu postavki moglo bi se izbjeći nadzornom pločom za privatnost, koja bi omogućila centralizaciju postavki i olakšala nadzor podataka korisnika.

b. Relevantne pravne odredbe

124. Kao što je već spomenuto[63], člankom 5. stavkom 1. točkom (a) OUZP-a propisuje se jedno od glavnih načela obrade osobnih podataka, prema kojem se osobni podaci obrađuju zakonito, pošteno i, što je posebno važno u ovom slučaju, transparentno s obzirom na ispitanika („zakonitost, poštenost i transparentnost"). U skladu s načelom pouzdanosti iz članka 5. stavka 2. OUZP-a voditelji obrade dužni su pokazati koje mjere poduzimaju kako bi osigurali ne samo zakonitost i poštenost nego i transparentnost svojih aktivnosti. Osim toga, u ovom su scenariju uporabe relevantna načela smanjenja količine podataka u skladu s člankom 5. stavkom 1. točkom (c) te tehničke i integrirane zaštite podataka u skladu s člankom 25. OUZP-a.

c. Obmanjujući obrasci dizajna

i. Obrasci koji se temelje na sadržaju

125. Prvi je problem na koji korisnici nailaze u ovom kontekstu to što ne znaju gdje su postavke zaštite podataka. Korisnici mogu pročitati obavijest o zaštiti podataka i odlučiti izmijeniti obradu njihovih osobnih podataka. To bi mogli poželjeti učiniti i bez čitanja obavijesti, samo na temelju redovitog korištenja društvenih medija, na primjer kad shvate da se informacije objavljene na platformi društvenih medija (npr. fotografija na plaži s obitelji) dijeli s neželjenom skupinom ljudi (npr. kolege s posla). U svakom slučaju, prema načelu transparentnosti postavke moraju biti lako dostupne i razumljive. To bi se moglo postići centralizacijom postavki podataka i privatnosti na jednom mjestu uz pomoć URL-a koji je razumljiv sam po sebi, kao što je [social-network.com]/data-settings.

126. S tim pitanjem povezano je nekoliko obrazaca dizajna koji korisnicima otežavaju pronalaženje postavki. Dizajneri platformi društvenih medija trebali bi nastojati izbjeći te obmanjujuće obrasce.

Preopterećenost – previše opcija (Prilog I., kontrolni popis 4.1.3.)

127. Postavke zaštite podataka moraju biti lako dostupne i smisleno poredane. Poželjno je da su postavke koje se odnose na isti aspekt zaštite podataka objedinjene na jednom istaknutom mjestu. U suprotnom će korisnici biti prisiljeni provjeravati i pregledavati prevelik broj stranica, što ih može opteretiti pri prilagodbi preferencija zaštite podataka. Ako im se nudi ***previše opcija***, možda neće moći donijeti odluku ili će previdjeti određene postavke te će naposljetku odustati ili zanemariti prilagodbu preferencija zaštite podataka. Time se krše načela transparentnosti i poštenosti. Konkretno, može se prekršiti članak 12. stavak 1. OUZP-a jer se otežava pristup određenoj kontroli zaštite podataka s obzirom na to da je raspoređena na više stranica ili jer je razlika između ponuđenih korisničkih opcija nejasna.

Primjer 36: Korisnici vjerojatno neće znati što učiniti ako izbornik platforme društvenih medija sadržava više kartica koje se odnose na zaštitu podataka: „zaštita podataka", „sigurnost", „sadržaj", „privatnost", „vaše preferencije".

128. U ovom primjeru naslovi kartica ne upućuju jasno na sadržaj koji će korisnici pronaći na povezanoj stranici niti pokazuju da se sve kartice odnose na zaštitu podataka, tim više što jedna od kartica nosi izričiti naziv „zaštita podataka". Zbog toga korisnici možda neće moći unijeti izmjene. Na primjer, ako korisnici žele ograničiti ili povećati broj osoba kojima su vidljive fotografije koje su prenijeli, nazivi kartica mogli bi ih navesti da kliknu na „sigurnost" ako misle da postoje određeni sigurnosni rizici zbog javne dostupnosti njihovih podataka, na „sadržaj" jer žele prilagoditi vidljivost svoje objave ili na „privatnost" jer se taj pojam izravno odnosi na opseg sadržaja koji ljudi žele podijeliti s drugima. To

[63] Vidjeti točke 1., 9., 10. i od 14. do 16.

znači da ti naslovi nisu dovoljno jasni s obzirom na radnje koje korisnici žele izvršiti. Na primjer, pojmovi „zaštita podataka" i „privatnost" često se koriste kao sinonimi i zato njihovo odvajanje u zasebne odjeljke posebno dovodi do zabune.

Držanje u neznanju – proturječne informacije (Prilog I., kontrolni popis 4.6.2.)

129. Kao što je već opisano u primjeru 12 i dodatno prikazano u sljedećem primjeru, u okviru postavki zaštite podataka korisnici mogu dobiti ***proturječne informacije***.

Primjer 37: Korisnik X isključuje korištenje svoje geolokacije u svrhu prikazivanja oglasa. Nakon što klikne na preklopni gumb koji to omogućuje, prikazuje se sljedeća poruka: *Isključili smo vašu geolokaciju, ali vaša lokacija će se i dalje koristiti.*

Preopterećenost – labirint pravila privatnosti (Prilog I., kontrolni popis 4.1.2.)

130. Kad korisnici promijene postavku zaštite podataka, prema načelu poštenosti pružatelji usluga društvenih medija dužni su obavijestiti korisnike i o drugim sličnim postavkama. Ako su takve postavke raspoređene na različitim, nepovezanim stranicama platforme društvenih medija, korisnicima će vjerojatno promaknuti jedna ili više značajki za nadzor određenog aspekta njihovih osobnih podataka. Korisnici očekuju da će se povezane postavke nalaziti jedna pored druge.

Primjer 38: Povezane teme, kao što su postavke dijeljenja podataka između pružatelja usluga društvenih medija i trećih strana, ne nalaze se na istom mjestu ili u neposrednoj blizini, već su raspoređene po različitim karticama u izborniku postavki.

131. Ne postoji univerzalni pristup u smislu prosječnog broja koraka za promjenu postavki koji je prihvatljiv korisnicima platformi društvenih medija. Međutim, zbog većeg broja koraka korisnici mogu odustati od unošenja promjene ili zanemariti neke dijelove, posebno ako žele unijeti više promjena. Takvim ograničavanjem volje korisnika krše se načela poštenosti iz članka 5. stavka 1. točke (a) OUZP-a. Osim toga, promjena postavki usko je povezana s ostvarivanjem prava ispitanika[64]. Promjena postavki podataka, kao što je ispravak imena ili brisanje godine završetka studija, može se smatrati ostvarivanjem prava na ispravak odnosno prava na brisanje tih konkretnih podataka. Zbog toga bi broj potrebnih koraka trebao biti što manji. Iako može varirati, prekomjeran broj koraka ometa korisnike i dovodi do povrede načela poštenosti, kao i članka 12. stavaka 1. i 2. OUZP-a.

Nestalnost – jezični diskontinuitet (Prilog I., kontrolni popis 4.5.4.)

132. Radi transparentnosti informacija dizajneri platformi društvenih medija moraju izbjegavati i obmanjujuće obrasce dizajna koji se temelje na sadržaju navedene u scenariju uporabe 2a, kao što je ***jezični diskontinuitet***. Ako stranice s postavkama (ili njihovi dijelovi) nisu dostupne na jeziku koji su korisnici odabrali za platformu društvenih medija, bit će im teško razumjeti što mogu promijeniti, a time i prilagoditi svoje preferencije.

Nestalnost – nedosljedno sučelje (Prilog I., kontrolni popis 4.5.3.)

133. U tom kontekstu nastaje još jedan problem kad platforme društvenih medija nude opcije koje pogoduju zaštiti podataka a da korisnici o tome nisu jasno informirani. To se može dogoditi kad se

[64] Vidjeti scenarije uporabe 4 i 5 u nastavku, tj. dijelove 3.4. i 3.5. ovih Smjernica.

uobičajeni obrazac dizajna na platformi društvenih medija iznenada promijeni. Takvo ***nedosljedno sučelje*** javlja se kad sučelje nije dosljedno u različitim kontekstima ili u skladu s očekivanjima korisnika. Zbog tih razlika korisnici možda neće pronaći željenu kontrolu ili informacije ili će koristiti elemente sučelja iz navike, iako ta interakcija dovodi do neželjenog izbora u smislu zaštite podataka.

Primjer 39: Na platformi društvenih medija devet od deset opcija postavki zaštite podataka prikazano je sljedećim redoslijedom:

– najrestriktivnija opcija (tj. dijeljenje najmanje podataka s drugima)

– ograničena opcija, ali manje restriktivna nego prva

– najmanje restriktivna opcija (tj. dijeljenje najviše podataka s drugima).

Korisnici platforme navikli su da im se postavke zaštite podataka prikazuju tim redoslijedom. Međutim, taj se redoslijed ne primjenjuje u posljednjoj postavci, u kojoj je izbor vidljivosti rođendana korisnika prikazan sljedećim redoslijedom:

– Prikaži moj cijeli datum rođenja: 15. siječnja 1929. (= najmanje restriktivna opcija)

– *Prikaži samo dan i mjesec: 15. siječnja* (= ograničena, ali ne i najrestriktivnija opcija)

– *Ne prikazuj drugima moj rođendan* (= najrestriktivnija opcija).

134. U primjeru su tri opcije u posljednjoj postavci prikazane drukčijim redoslijedom nego u prethodnim postavkama. Korisnici koji su već promijenili svoje druge postavke vjerojatno su navikli na „uobičajeni" redoslijed prvih devet postavki. Kad dođu do posljednje postavke, toliko su navikli na taj redoslijed da instinktivno biraju prvu opciju uz pretpostavku da je ona najrestriktivnija. Toliko različit raspored opcija jedne postavke zaštite podataka u odnosu na druge postavke na istoj platformi društvenih medija ***nedosljedno je sučelje*** jer remeti navike i očekivanja korisnika. Zbog toga se korisnici mogu zbuniti ili misliti da su odabrali što su željeli, iako zapravo nisu.

ii. Obrasci koji se temelje na sučelju

135. Drugi problem koji se javlja u kontekstu postavki zaštite podataka jest taj da one mogu biti u suprotnosti s načelom integrirane zaštite podataka. Člankom 25. stavkom 1. OUZP-a propisuje se da je voditelj obrade dužan provoditi odgovarajuće mjere za primjenu načela zaštite podataka, kao što je smanjenje količine podataka (članak 5. stavak 1. točka (c) OUZP-a). Te se odredbe ne poštuju ako je u postavkama dijeljenja osobnih podataka unaprijed odabrana jedna od invazivnijih opcija umjesto najmanje invazivne.

Preskakanje – obmanjujući komfor (Prilog I., kontrolni popis 4.2.1.)

Primjer 40: Među opcijama vidljivosti podataka „vidljivo meni", „mojim najbližim prijateljima" „svim mojim vezama", i „javno", unaprijed je postavljena srednja opcija „svim mojim vezama". To znači da svi korisnici povezani s osobom mogu vidjeti njezine objave, kao i sve informacije unesene pri registraciji na platformu društvenih medija, na primjer e-adresu ili datum rođenja.

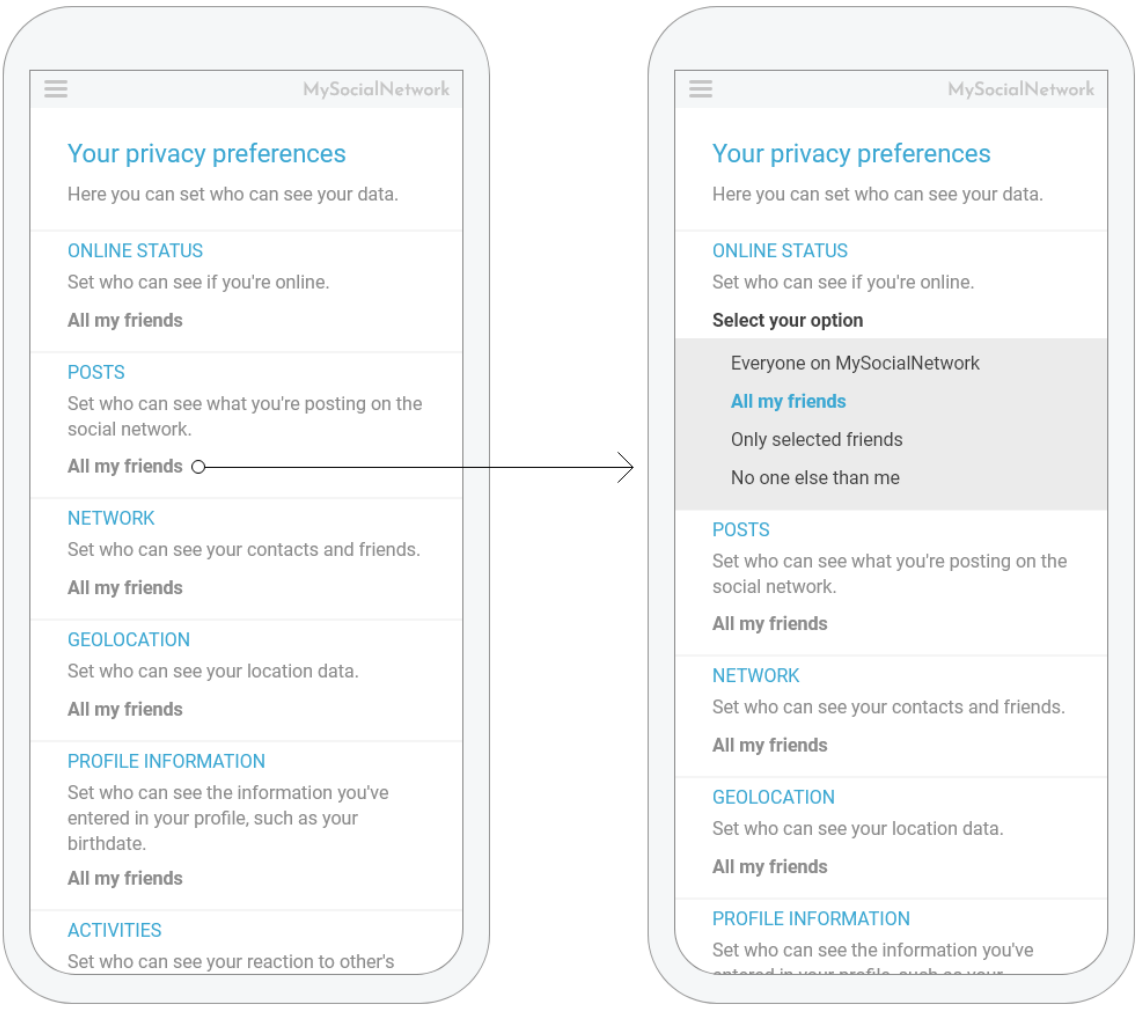
136. Pružatelji usluga društvenih medija mogu tvrditi da najmanje invazivna postavka nije u skladu s ciljem korisnika određene platforme društvenih medija, na primjer da ih nepoznate osobe pronađu kako bi sklopili novo prijateljstvo, upoznali partnera ili pronašli posao. Iako to može vrijediti za određene

postavke, pružatelji usluga društvenih medija moraju imati na umu da to što korisnici prenose određene podatke na mrežu ne znači da pristaju na dijeljenje tih podataka s drugima[65]. Ako pružatelji usluga društvenih medija automatski odstupaju od zaštite podataka, moraju na odgovarajući način o tome obavijestiti korisnike. To znači da korisnici moraju znati koja je zadana postavka, da su dostupne manje invazivne opcije i gdje na platformi mogu promijeniti postavku. U danom primjeru to znači da bi korisnicima, ako je za sadržaj koji aktivno objavljuju na platformi društvenih medija unaprijed postavljena opcija „mojim najbližim prijateljima", trebalo pokazati gdje mogu promijeniti tu postavku. Međutim, unaprijed postavljena opcija vidljivosti „svim korisničkim vezama" (ili čak široj javnosti) primjer je ***obmanjujućeg komfora***, posebno ako se primjenjuje na podatke koje je pružatelj usluga društvenih medija zatražio od korisnika radi izrade računa, kao što su e-adresa ili datum rođenja. Kako je opisano u scenariju uporabe 1 u točki 55., tom se praksom krši članak 25. stavak 2. OUZP-a.

[65] Na primjer datum rođenja, vidjeti točku 58.

Stimuliranje – skrivanje na vidljivom mjestu (Prilog I., kontrolni popis 4.3.2.)

137. U kontekstu odabira opcija zaštite podataka obmanjujući obrasci dizajna ***skrivanje na vidljivom mjestu*** i ***obmanjujući komfor*** često se javljaju zajedno, što je vidljivo iz postupka registracije iz primjera 9 i u primjeru u nastavku, u kojem korisnici žele promijeniti svoje preferencije zaštite podataka tijekom korištenja društvenih medija.



Primjer 41: U ovom primjeru korisnici koji žele upravljati vidljivošću svojih podataka moraju otvoriti karticu „Preferencije privatnosti". Ondje su navedene informacije za koje mogu odabrati svoje preferencije. Međutim, informacije su prikazane tako da nije jasno kako promijeniti postavke. Naime, korisnici moraju kliknuti na postojeću opciju vidljivosti da bi otvorili padajući izbornik u kojem mogu odabrati željenu opciju.

138. Iako je u toj kartici moguće promijeniti preferencije, opcija je ***skrivena na vidljivom mjestu*** jer padajući izbornik nije izravno vidljiv i korisnici moraju pogoditi da će se klikom na postojeću opciju otvoriti dodatna opcija. Nije prisutan uobičajeni vizualni pokazatelj (podcrtani tekst, strelica prema dolje) da postoji mogućnost interakcije i otvaranja padajućeg izbornika. Ta je konkretna praksa nepoštena prema korisnicima i mogla bi dovesti do opće neusklađenosti s načelom poštenosti iz članka 5. stavka 1. točke (a) OUZP-a. Osim toga, ako su opcije automatski unaprijed odabrane, prisutan je i obmanjujući obrazac dizajna poznat kao ***obmanjujući komfor***, kako je već opisano u točki 128.

Nestalnost – dekontekstualizacija (Prilog I., kontrolni popis 4.5.2.)

139. ***Dekontekstualizacija*** podrazumijeva da se informacija ili kontrola povezana sa zaštitom podataka nalazi na stranici koja je izvan konteksta, tako da je korisnici vjerojatno neće pronaći jer ne bi bilo intuitivno tražiti je na toj stranici.

> **Primjer 42:** U korisničkom računu teško je pronaći postavke zaštite podataka jer na prvoj razini ne postoji stavka izbornika s nazivom ili naslovom koji bi usmjerio korisnike prema njima. Korisnici moraju pregledavati druge podizbornike, kao što je „Sigurnost".

140. U ovom primjeru korisnike se ne usmjerava prema postavkama zaštite podataka jer se ne koriste smisleni i jasni pojmovi koji bi naznačili gdje se one nalaze na platformi društvenih medija. Pojam „Sigurnost" obuhvaća samo dio očekivanih postavki zaštite podataka. Zbog toga nije intuitivno da korisnici takve postavke traže u tom izborniku. Taj manjak transparentnosti nepotrebno otežava pristup informacijama i može se smatrati da je u suprotnosti s člankom 12. stavkom 1. OUZP-a, a potencijalno i s njegovim člankom 12. stavkom 2. ako se te postavke odnose na ostvarivanje prava.

> **Primjer 43:** Promjena postavke otežana je jer u verziji platforme društvenih medija za računala gumb „Spremi" za registriranje promjena nije vidljiv za sve opcije, već samo na vrhu podizbornika. Korisnici će ga vjerojatno previdjeti i pogrešno pretpostaviti da se njihove postavke automatski spremaju, stoga prelaze na drugu stranicu a da nisu kliknuli na gumb „Spremi". Taj problem ne pojavljuje se u aplikaciji i mobilnim verzijama. Stoga dodatno zbunjuje korisnike koji prelaze s mobilne verzije ili aplikacije na verziju za računala i koji bi mogli pomisliti da svoje postavke mogu mijenjati samo u mobilnoj verziji ili aplikaciji.

141. Nakon što korisnici pronađu postavke zaštite podataka i prilagode svoje preferencije, u tome ih se ne smije sprečavati. Nakon što korisnici unesu promjenu, način njezina spremanja mora biti očit bez obzira na to sprema li se čim korisnici prilagode postavku ili je potrebna potvrda klikom na određeni element sučelja kao što je gumb „Spremi". Osim toga, prema načelu poštenosti iz članka 5. stavka 1. točke (a) OUZP-a pružatelji usluga društvenih medija moraju biti konzistentni na cijeloj svojoj platformi, a posebno na različitim uređajima. To načelo nije zadovoljeno ako se na sučelju primjenjuje obmanjujući obrazac dizajna, kako je opisano u navedenim primjerima.

d. Primjeri dobre prakse

Registar zaštite podataka: radi lakšeg snalaženja u različitim dijelovima izbornika korisnicima stavite na raspolaganje lako dostupnu stranicu na kojoj će moći pristupiti svim radnjama (npr. postavke) i informacijama povezanima sa zaštitom podataka. Ta stranica može se nalaziti u glavnom navigacijskom izborniku pružatelja usluga društvenih medija, korisničkom računu, pravilima zaštite privatnosti itd.

Skupne opcije: grupiranje opcija koje imaju istu svrhu obrade kako bi ih korisnici lakše mijenjali, pri čemu i dalje mogu unositi granularne izmjene. Ako platforme društvenih medija nude skupne opcije, one ne bi smjele sadržavati neočekivane ili nepovezane elemente (npr. elementi s različitom svrhom). Ako je za obradu potrebna privola, skupne opcije moraju biti u skladu sa Smjernicama EDPB-a o privoli, posebno točkama od 42. do 44.

Prečaci: vidjeti definiciju u scenariju uporabe 1 (str. 22) *(npr. kad se korisnici obavještavaju o određenom aspektu obrade, pozivaju se da postave svoje povezane preferencije podataka na odgovarajućoj stranici s postavkama / nadzornom pločom)*.

URL koji je razumljiv sam po sebi: za stranice koje se odnose na postavke ili informacije povezane sa zaštitom podataka trebalo bi koristiti internetsku adresu koja jasno odražava njihov sadržaj. Na primjer, za stranicu na kojoj je centraliziran nadzor zaštite podataka može se koristiti URL kao što je [social-network.com]/data-settings.

Usklađeni tekst: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Navođenje definicija: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Korištenje primjera: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Fiksna navigacija (eng. *sticky navigation*): vidjeti definiciju u scenariju uporabe 2a (str. 28).

Obavijesti: vidjeti definiciju u scenariju uporabe 2c (str. 32).

Objašnjavanje posljedica: vidjeti definiciju u scenariju uporabe 2c (str. 32).

Dosljednost na različitim uređajima: vidjeti definiciju u scenariju uporabe 3a (str. 39).

3.4. Prava na društvenim medijima prava ispitanika

Scenarij uporabe 4: kako osigurati odgovarajuće funkcije za ostvarivanje prava ispitanika

a. Opis konteksta

142. Korištenje platforme društvenih medija podrazumijeva iskorištavanje njezinih funkcija u skladu sa svrhama koje je naveo pružatelj usluga društvenih medija. To znači i da korisnici trebaju moći ostvarivati svoja prava zaštite podataka. Riječ je o ključnim elementima zaštite podataka i nadzora nad vlastitim informacijama, bez obzira na to pružaju li ispitanici podatke izravno i svjesno ili korištenjem usluge ili uređaja ili se oni izvode na temelju analize podataka koje je pružio ispitanik[66]. Budući da platformom cirkulira velika količina osobnih podataka, korisnicima se mora omogućiti jasan i intuitivan nadzor nad njihovim podacima na temelju prava predviđenih OUZP-om. EDBP je objasnio te pojmove u nekoliko dokumenata sa smjernicama[67]. Ostvarivanje prava mora biti dostupno od početka do kraja korištenja platforme, a u nekim slučajevima čak i nakon što korisnici odluče napustiti platformu, a voditelj obrade još nije uklonio njihove podatke. Ostvarivanje prava ispitanika koja se odnose na obradu osobnih podataka mora se omogućiti i osobama koje nisu korisnici platforme. Dakako, u određenim slučajevima nisu dostupna sva prava ispitanika, ovisno o pravnoj osnovi za obradu podataka. Zato bi pružatelj usluga društvenih medija trebao jasno obrazložiti i zašto određena prava nisu primjenjiva i zašto neka od njih mogu biti ograničena. Kao što je već spomenuto i u prethodnim poglavljima, ostvarivanje prava mora postati učinkovito. Automatizacija i druge funkcije platformi društvenih medija trebale bi olakšati ostvarivanje prava.

b. Relevantne pravne odredbe

143. U OUZP-u je opisano sedam prava koja ispitanici mogu ostvariti u skladu s određenim uvjetima (npr. pravna osnova za obradu). Članak 15. OUZP-a ispitanicima omogućuje da doznaju obrađuju li se osobni

[66] Vidjeti Smjernice Radne skupine iz članka 29. o pravu na prenosivost podataka na temelju Uredbe 2016/679, WP 242 rev.01, str. 10 https://ec.europa.eu/newsroom/article29/items/611233/en.

[67] Smjernice o pravu na prenosivost podataka i Smjernice EDPB-a 5/2019 o kriterijima prava na zaborav u slučajevima internetskih pretraživača u skladu s Općom uredbom o zaštiti podataka (1. dio) – verzija donesena nakon javnog savjetovanja, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_hr.

podaci koji se odnose na njih i da dobiju pristup tim podacima, tj. da dobiju dodatne informacije o njihovoj obradi, kao i kopiju tih podataka. U članku 16. OUZP-a opisuje se pravo na ispravak, koje ispitanicima omogućuje ažuriranje osobnih podataka koje voditelj obrade obrađuje. Pravo na brisanje u skladu s člankom 17. OUZP-a ispitanicima omogućuje da ishode brisanje osobnih podataka koji se na njih odnose. Pravo na ograničenje obrade u skladu s člankom 18. OUZP-a predviđa mogućnost da ispitanici privremeno zaustave obradu njihovih osobnih podataka. Člankom 20. OUZP-a uvodi se pravo na prenosivost podataka, koje ispitanicima omogućuje da zaprime svoje osobne podatke i prenesu ih drugom voditelju obrade[68]. Ispitanici imaju i pravo na prigovor na obradu njihovih osobnih podataka kako je utvrđeno u članku 21. OUZP-a. Naposljetku, na temelju članka 22. OUZP-a ispitanici imaju pravo da se na njih ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi[69].

144. EDPB naglašava da se neće sva prava primjenjivati na svaku platformu društvenih medija, već će to ovisiti o njezinoj pravnoj osnovi, svrhama obrade osobnih podataka i vrstama pruženih usluga. Voditelj obrade trebao bi objasniti razlike u skladu s člankom 12. OUZP-a. To znači da bi informacije o primjenjivim pravima, uključujući razloge zbog kojih se određena prava ne primjenjuju, trebale biti sažete i jasne korisnicima. Takvo objašnjenje moglo bi ograničiti količinu komunikacije s korisnicima kad pokušavaju ostvariti neka od tih prava. Ostvarivanje prava trebalo bi biti jednostavno i pristupačno u skladu s člankom 12. stavkom 2., a odgovor bi trebalo dostaviti bez nepotrebnog odgađanja u skladu s člankom 12. stavkom 3. OUZP-a. Slično tomu, platforma društvenih medija trebala bi objasniti zašto se određeni zahtjevi ne mogu ispuniti i obavijestiti o mogućnosti podnošenja prigovora imenovanom nadzornom tijelu u skladu s člankom 12. stavkom 4. OUZP-a. Sljedeći obmanjujući obrasci dizajna stoga možda neće biti primjenjivi na sva navedena prava. Pravo na brisanje podrobno se razmatra u sljedećem poglavlju.

c. Obmanjujući obrasci dizajna

i. Obrasci koji se temelje na sadržaju

Ometanje – slijepa ulica (Prilog I., kontrolni popis 4.4.1.)

145. Obmanjujući obrazac dizajna poznat kao ***slijepa ulica*** može izravno utjecati na jednostavnost pristupa ostvarivanju prava. Ako su poveznice na značajke za ostvarivanje prava prekinute ili nedostaju jasna objašnjenja o tome kako ostvariti određeno pravo, korisnici ga neće moći pravilno ostvariti, čime se krši članak 12. stavak 2. OUZP-a.

Primjer 44: Korisnik klikne na „Želim ostvariti svoje pravo pristupa" u obavijesti o zaštiti privatnosti, ali se umjesto toga preusmjeri na svoj profil, koji ne sadržava nikakve značajke povezane s ostvarivanjem prava.

146. U navedenom primjeru obmanjujućeg obrasca dizajna ističe se potreba da se korisnicima omogući jasno i intuitivno ostvarivanje prava u skladu s člankom 12. stavcima 1. i 2. OUZP-a jer ih inače možda neće moći ostvariti. Nije dovoljno potvrditi korisnicima da imaju prava ispitanika u skladu s člankom 12. stavkom 1. OUZP-a (uključujući način komunikacije), a posebno u skladu s člankom 13. stavkom 2. točkom (b) i člankom 14. stavkom 2. točkom (c) OUZP-a. Korisnicima bi trebalo omogućiti i da ih lako ostvare, po mogućnosti s pomoću opcije ugrađene u sučelje platforme, na primjer namjenskog obrasca. To bi ujedno poboljšalo korisničko iskustvo na platformi jer se pružatelj usluga kombiniranjem

[68] To je pravo dodatno razrađeno u Smjernicama o pravu na prenosivost podataka.
[69] Vidjeti i Smjernice Radne skupine iz članka 29. o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, WP251rev.01, str. 19 i dalje, https://ec.europa.eu/newsroom/article29/items/612053/en.

ostvarivanja prava s drugim funkcijama usluge prilagodio očekivanjima korisnika u pogledu zakonite obrade osobnih podataka i nadzora nad njihovim podacima. Ako usluga platforme društvenih medija omogućuje dvosmjernu komunikaciju među korisnicima, kao i između voditelja obrade i korisnika, nema razloga da voditelj obrade ograniči svoj komunikacijski kanal za jednostavnije podnošenje zahtjeva ispitanika na zasebno sredstvo komunikacije kao što je e-pošta. S druge strane, ispitanike ne bi trebalo prisiljavati da pristupe platformi kako bi komunicirali s voditeljem obrade[70]. Osim toga, voditelji obrade ne smiju ograničiti to pravo ispitanika na pravo na kopiju, već su dužni korisnicima koji zatraže pristup svojim podacima pružiti i informacije navedene u članku 15. stavku 1. OUZP-a[71].

Nestalnost – jezični diskontinuitet (Prilog I., kontrolni popis 4.5.4.)

Primjer 45: Kad se klikne na poveznicu za ostvarivanje prava ispitanika, sljedeće informacije nisu navedene na nekom od službenih jezika države korisnika, iako se usluga pruža na tom jeziku. Korisnike se umjesto toga preusmjerava na stranicu na engleskom jeziku.

147. Imajući na umu načelo transparentnosti iz članka 5. stavka 1. točke (a) i članka 12. stavka 1. OUZP-a, korisnici moraju dobiti sve informacije o svojim pravima u jasnom, jednostavnom i razumljivom obliku. On mora biti prilagođen i lokaciji korisnika i jeziku te zemlje ili jurisdikciji u kojoj se usluga nudi. To što korisnici potvrđuju svoje poznavanje stranog jezika ni na koji način ne oslobađa voditelja obrade od obveza. Isto vrijedi i u situacijama kad se iz aktivnosti korisnika može zaključiti da poznaju druge jezike. Informacije bi trebale biti relevantne i korisne za korisnike koji ostvaruju svoja prava.

Držanje u neznanju – dvosmisleni tekst ili informacije (Prilog I., kontrolni popis 4.6.3.)

148. U kontekstu prava ispitanika korisnici mogu naići i na obmanjujući obrazac dizajna poznat kao ***dvosmisleni tekst ili informacije***, kako je prikazano u sljedećem primjeru.

Primjer 46: Na platformi društvenih medija ne navodi se izričito da korisnici u EU-u imaju pravo podnijeti prigovor nadzornom tijelu, već se samo navodi da u nekim zemljama postoje tijela za zaštitu podataka s kojima pružatelj usluga društvenih medija surađuje u vezi s prigovorima. Pritom nije navedeno o kojim je zemljama riječ.

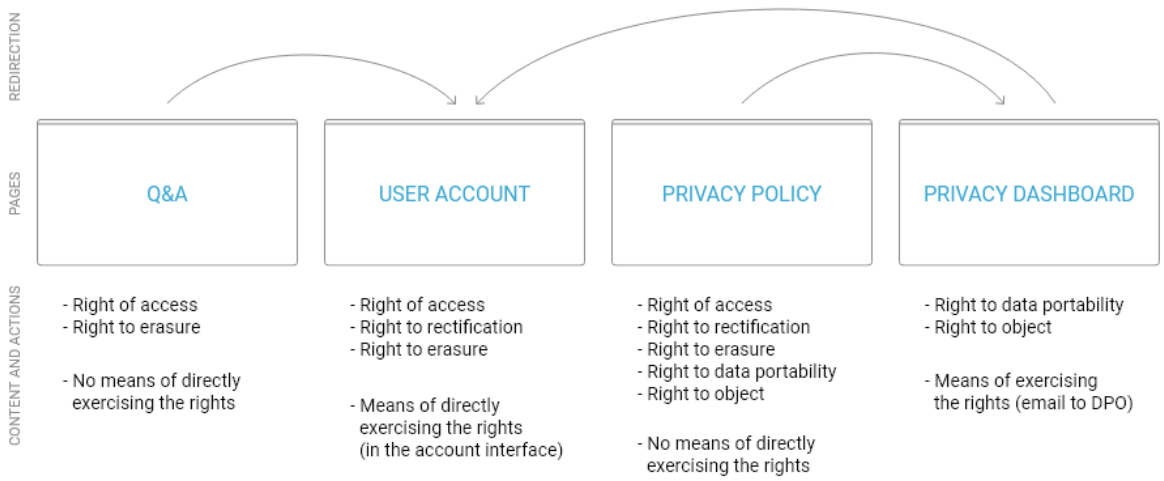
149. Osim toga, pružatelji usluga društvenih medija trebaju izbjegavati obmanjujući obrazac dizajna ***dvosmisleni tekst ili informacije*** kad informiraju ispitanike o njihovim pravima. Ako se informacije pružaju tako da korisnici nisu sigurni kako će se njihovi podaci obrađivati ili kako ostvariti određeni nadzor nad svojim podacima, a time i svoja prava, krši se načelo transparentnosti. Osim toga, nejasan tekst nije pisan sažetim jezikom kako je propisano člankom 12. stavkom 1. OUZP-a i zbog toga informacije koje se pružaju ispitaniku mogu biti nepotpune, što bi se moglo smatrati povredom članka 13. OUZP-a. Navedeni primjer sadržava i povredu članka 13. stavka 2. točke (d) OUZP-a, kojim se propisuje da su voditelji obrade dužni pružiti ispitanicima informacije o njihovu pravu na podnošenje prigovora nadzornom tijelu. To je ujedno u suprotnosti s člankom 12. stavkom 2. OUZP-a jer pružatelj usluga društvenih medija ne olakšava ostvarivanje prava na podnošenje prigovora.

[70] Vidjeti Smjernice EDPB-a 01/2022 o pravima ispitanika – pravo na pristup, točku 136., verziju 1.0, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.
[71] Vidjeti Smjernice EDPB-a 01/2022, točke 131., 142. i 145.

ii. Obrasci koji se temelje na sučelju

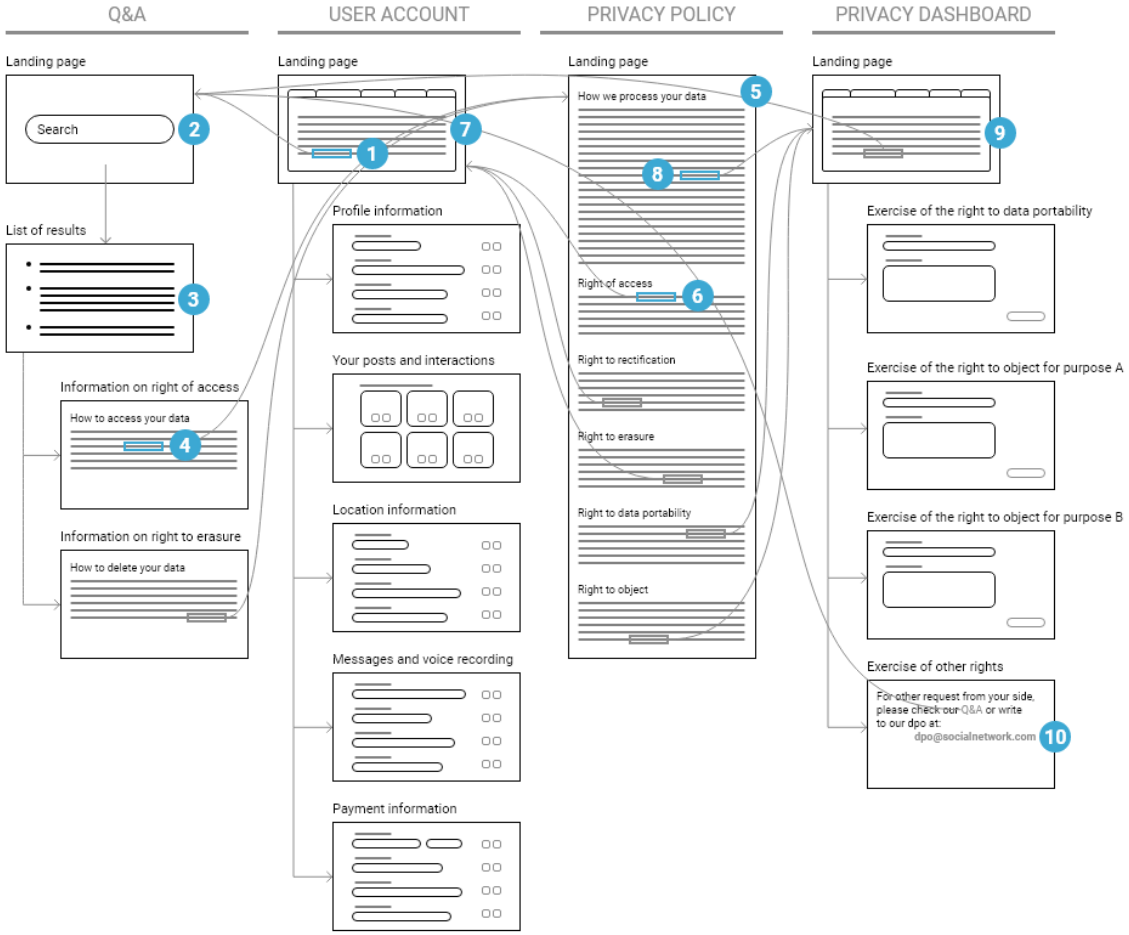
Preopterećenost – labirint pravila privatnosti (Prilog I., kontrolni popis 4.1.2.)

150. Kako je opisano u scenariju uporabe 3b, broj koraka potrebnih za dobivanje relevantnih informacija o zaštiti podataka ne smije biti prekomjeran, kao ni broj koraka za ostvarivanje prava ispitanika[72]. Korisnici bi stoga uvijek trebali moći brzo pristupiti mjestu za ostvarivanje prava bez obzira na polazišnu točku i lokaciju te značajke na platformi društvenih medija. Pružatelji usluga društvenih medija trebali bi pažljivo razmisliti o situacijama u kojima bi korisnici željeli ostvariti svoja prava i osmisliti pristup mjestu na kojem to mogu učiniti. To znači da se na platformi društvenih medija može osmisliti i staviti na raspolaganje više putova za pristup određenom pravu ispitanika. Međutim, svaki bi put trebao olakšati pristup ostvarivanju prava i ne bi smio ometati drugi put. U suprotnom bi se smatralo da je riječ o obmanjujućem obrascu dizajna poznatom kao ***labirint pravila privatnosti***, kako je opisano u primjerima 47 i 48, koji je protivan članku 12. stavku 2. OUZP-a.



Primjer 47: U ovom su primjeru informacije o pravima zaštite podataka navedene na najmanje četiri stranice. Iako pravila zaštite privatnosti sadržavaju informacije o svim pravima, ne postoji opcija preusmjeravanja na odgovarajuće stranice za svako pravo. S druge strane, kad se korisnici prijave na svoj račun, neće pronaći nikakve informacije o pravima koja mogu ostvariti. Zbog ***labirinta pravila privatnosti*** korisnici su prisiljeni pretraživati velik broj stranica kako bi doznali gdje mogu ostvariti svako pravo i, ovisno o pretraživanju, možda nisu ni upoznati sa svim svojim pravima.

[72] Vidjeti točku 123.



Primjer 48: U ovom primjeru korisnik želi ažurirati neke osobne podatke, ali ne zna kako to učiniti na svojem računu. Klikne na poveznicu (1) koja ga preusmjerava na stranicu s pitanjima i odgovorima na kojoj unese svoje pitanje (2). Pojavi se nekoliko rezultata (3). Neki od njih povezani su s pravima pristupa i uklanjanja. Nakon provjere svih rezultata klikne (4) na poveznicu na stranici „Kako pristupiti svojim podacima". Preusmjerava se na pravila zaštite privatnosti (5). Ondje pronalazi informacije o dodatnim pravima. Nakon što pročita te informacije, klikne (6) na poveznicu za ostvarivanje prava na ispravak, koja ga preusmjerava na korisnički račun (7). Nezadovoljan korisnik vraća se na pravila zaštite privatnosti i klikne na opću poveznicu „Pošaljite nam zahtjev" (8). Poveznica vodi do njegove nadzorne ploče za privatnost (9). Budući da nijedna od dostupnih opcija ne odgovara njegovim potrebama, korisnik naposljetku otvara stranicu (10) „Ostvarivanje drugih prava", na kojoj konačno pronalazi adresu za kontakt.

151. U oba primjera opisani su posebno dugi i zamorni putovi za ostvarivanje prava. Ako se značajke za ostvarivanje različitih prava ne nalaze na istom mjestu, nego je dostupna stranica na kojoj su navedena sva prava ispitanika, ta bi stranica trebala usmjeravati korisnike na svako od tih mjesta, a ne samo na jedno ili neka od njih, kako je prikazano u primjeru 47. U drugom primjeru korisnik ne uspijeva pronaći značajku za jednostavno ostvarivanje određenog prava, odnosno prava na ispravak, jer na korisničkom računu, gdje se ono obično ostvaruje, nije dostupna značajka za obavljanje te radnje. Kad pokuša

pronaći drugi način ostvarivanja tog prava, ne uspijeva pronaći odgovarajuću opciju i prisiljen je koristiti opću značajku na nadzornoj ploči privatnosti.

152. Ako postoji više putova za ostvarivanje prava, korisnicima bi uvijek trebalo biti lako pronaći pregled prava ispitanika. Pravila zaštite privatnosti trebala bi biti jasna i mogla bi služiti kao točka za pristup stranicama na kojima korisnici mogu ostvariti svoja prava. U tom bi dokumentu trebala biti navedena sva primjenjiva prava. Ako je koje od njih nedostupno zbog pravnih ili tehničkih ograničenja, i to bi trebalo objasniti kako bi korisnici bili propisno informirani. Razumijevanje ograničenja postupaka obrade bez obzira na to proizlaze li iz njihove osnove ili zaštitnih mjera koje su donijeli voditelji obrade ne pomaže samo korisnicima, nego i smanjuje broj slučajeva u kojima pružatelj usluga društvenih medija mora objašnjavati zašto ne može ispuniti zahtjev korisnika za ostvarivanje prava ispitanika.

Stimuliranje – skrivanje na vidljivom mjestu (Prilog I., kontrolni popis 4.3.2.)

153. Jedva vidljive relevantne informacije ili poveznice kao posljedica primjene obmanjujućeg obrasca dizajna poznatog kao ***skrivanje na vidljivom mjestu***isto tako mogu utjecati na mogućnost korisnika da pristupi mjestu gdje može ostvariti svoje pravo.

Primjer 49: U odlomku pravila zaštite privatnosti s podnaslovom „Pravo pristupa” objašnjava se da korisnici imaju pravo dobiti informacije u skladu s člankom 15. stavkom 1. OUZP-a. Međutim, spominje se samo mogućnost korisnika da dobiju kopiju svojih osobnih podataka. Nije dostupna izravna poveznica za dobivanje kopije u okviru prava pristupa u skladu s člankom 15. stavkom 3. OUZP-a. Umjesto toga, prve tri riječi u rečenici „Možete dobiti kopiju svojih osobnih podataka” blago su podcrtane. Kad korisnici zadrže pokazivač miša iznad tih riječi, prikazuje se mali okvir s poveznicom na postavke.

154. U skladu s prethodnim odjeljkom sve značajke koje voditelj obrade uvede za ostvarivanje prava trebale bi biti lako dostupne. Važnost tog pravila ne smije se podcijeniti. Postupak voditelja obrade kako je prethodno opisan može se tumačiti samo kao pokušaj da se spriječi ostvarivanje prava korisnika, čime se krši članak 12. stavak 2. OUZP-a. Voditelji obrade ne bi smjeli kočiti ostvarivanje takvog zahtjeva bez obzira na razloge. U konkretnom slučaju nadzorno tijelo moglo bi pomnijim ispitivanjem utvrditi da je riječ o povredi OUZP-a, što bi dovelo do sankcija za voditelja obrade.

Nestalnost – nedosljedno sučelje (Prilog I., kontrolni popis 4.5.3.)

Primjer 50: Platforma društvenih medija nudi različite verzije (računalo, aplikacija, mobilni preglednik). U svakoj se verziji postavke (za pristup/prigovor itd.) prikazuju s različitim simbolom, što zbunjuje korisnike koji upotrebljavaju više verzija.

155. Ako se na sučeljima različitih uređaja iste informacije prenose različitim vizualnim oznakama, korisnicima će vjerojatno trebati više vremena ili će im biti teško pronaći kontrole koje su im poznate s drugog uređaja. U gornjem primjeru to se događa jer se za usmjeravanje korisnika na postavke koriste različiti simboli ili ikone. Može se smatrati da je takvo zbunjivanje korisnika protivno načelu olakšavanja ostvarivanja prava ispitanika kako je navedeno u članku 12. stavku 2. OUZP-a.

Ometanje – dulje trajanje od nužnog (Prilog I., kontrolni popis 4.4.2.)

156. Naposljetku, svaki pokušaj da ostvarivanje prava traje ***dulje nego što je nužno*** može se smatrati protivnim OUZP-u.

> **Primjer 51:** Kad korisnik odluči izbrisati ime i mjesto svoje srednje škole ili upućivanje na događaj kojem su prisustvovali i koji su podijelili, pojavljuje se drugi prozor u kojem se traži potvrda tog izbora („Želite li zaista to učiniti? Zašto to želite učiniti?").

157. Kao i broj slojeva u pravilima zaštite privatnosti (scenarij uporabe 2a) i broj koraka za pristupanje postavci ili njezinu promjenu (scenarij uporabe 3b), broj koraka ili klikova potrebnih kako bi korisnik ostvario određeno pravo ne bi trebao biti prekomjeran. To dakako ovisi o složenosti postupaka voditelja obrade uzimajući u obzir specifični kontekst. Međutim, bilo bi nerazumno zahtijevati da korisnici poduzmu velik broj nepotrebnih radnji kako bi dovršili ostvarivanje svojeg prava. Na primjer, korisnike ne bi trebalo obeshrabrivati dodatnim pitanjima, na primjer žele li zaista ostvariti to pravo ili koji su razlozi za takav zahtjev. U većini slučajeva trebali bi moći samo ostvariti svoje pravo a da se pritom njihova motivacija ne dovodi u pitanje. Takva praksa, prikazana u prethodnom primjeru, može se smatrati protivnom članku 12. stavku 2. OUZP-a jer voditelj obrade nepotrebnim koracima otežava ostvarivanje prava. Naravno, to ne isključuje mogućnost da voditelj obrade naknadno prikupi povratne informacije postavljanjem dodatnih pitanja radi poboljšanja usluge. Ako se ta pitanja postave naknadno, odgovori na njih ovisili bi isključivo o volji korisnika i ne bi se smatrali zahtjevom za ostvarivanje prava.

d. Primjeri dobre prakse

Obrazac za ostvarivanje prava: da biste korisnicima olakšali ostvarivanje njihovih prava iz OUZP-a, osigurajte poseban obrazac koji će korisnicima pomoći da razumiju svoja prava i usmjeriti ih pri provedbi takvih zahtjeva.

Prečaci: vidjeti definiciju u scenariju uporabe 1 (str. 22) (npr. *osigurajte poveznicu na opciju uklanjanja računa u korisničkom računu*).

Usklađeni tekst: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Navođenje definicija: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Korištenje primjera: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Fiksna navigacija (eng. *sticky navigation*): vidjeti definiciju u scenariju uporabe 2a (str. 28).

Objašnjavanje posljedica: vidjeti definiciju u scenariju uporabe 2c (str. 32).

Dosljednost na različitim uređajima: vidjeti definiciju u scenariju uporabe 3a (str. 39).

Registar zaštite podataka: vidjeti definiciju u scenariju uporabe 3b (str. 45).

Odnos kontrola zaštite podataka: vidjeti definiciju u scenariju uporabe 3b (str. 45).

3.5. Vrijeme je za oproštaj: zatvaranje računa na društvenim medijima

Scenarij uporabe 5: pauziranje računa / brisanje svih osobnih podataka

a. Opis konteksta i relevantne pravne odredbe

158. Kraj životnog ciklusa računa odnosi se na situaciju kad korisnici odluče napustiti društvenu mrežu. U takvoj situaciji korisnici obično odluče trajno napustiti platformu društvenih medija. Međutim, često postoji i opcija privremenog onemogućavanja računa i pauziranja usluge. Pravne posljedice obiju odluka razlikuju se i opisane su u nastavku.

i. Trajno brisanje računa

159. Odluka o trajnom napuštanju platforme društvenih medija popraćena je pravom na brisanje iz članka 17. stavka 1. točke (a) OUZP-a. U tom se kontekstu riječ „uklanjanje" upotrebljava češće od riječi „brisanje".

160. Riječ „brisanje" nije pravno definirana u članku 17. OUZP-a i spominje se samo kao oblik obrade u članku 4. točki 2. OUZP-a. Brisanje se općenito može shvatiti kao (činjenična) nemogućnost percepcije informacija o ispitaniku koje su prethodno bile sadržane u podacima koji se brišu. Nakon brisanja više ne smije biti moguće da itko percipira predmetne informacije bez nerazmjernog napora.

161. Anonimizacija je još jedan način trajnog prekida poveznice s osobom. Drugim riječima, primjenom tehnika anonimizacije nastoji se onemogućiti utvrđivanje identiteta ispitanika. Anonimizacija znači i da pravna načela u području zaštite podataka, kao što je načelo ograničavanja svrhe, više nisu primjenjiva (vidjeti uvodnu izjavu 26. četvrtu i petu rečenicu).

162. U skladu s člankom 12. stavkom 2. OUZP-a voditelj obrade dužan je olakšati ostvarivanje prava ispitanika iz članaka od 15. do 22. To znači da se ne smiju stvarati materijalne ili formalne prepreke ostvarivanju prava ispitanika. Ako je ostvarivanje prava na brisanje otežano bez stvarnog razloga, riječ je o povredi OUZP-a. Iako postoji valjan razlog da pružatelji usluga društvenih medija objektivno objasne posljedice, na primjer uklanjanje svih osobnih podataka, i zatraže od ispitanika da potvrde taj izbor[73], i u tom scenariju treba izbjegavati nepotrebne prepreke. Iz toga na primjer proizlazi da svako razdoblje odgode između zahtjeva korisnika za uklanjanja računa i stvarnog uklanjanja računa mora biti razmjerno. To razdoblje stoga ne smije biti predugo uzimajući u obzir odgodu trenutnog brisanja zbog nužnih tehničkih razloga, kao i kratko razdoblje nakon pokretanja postupka uklanjanja računa u kojem korisnici preispituju svoju odluku. Iako treba poštovati slobodu korisnika da promijene mišljenje, pružatelji usluga društvenih medija ne smiju pokušati izazvati takvu promjenu poticanjem korisnika da se vrate jer bi se i to smatralo preprekom pravu korisnika na uklanjanje. U razdoblju odgode postupak uklanjanja mogao bi se prekinuti u nekim slučajevima, npr. kad se korisnik ponovno prijavi. Ako se uklanjanje ne može dovršiti, potrebno je o tome obavijestiti korisnika i dati mu upute kako da dovrši uklanjanje.

163. Odluka o napuštanju platforme društvenih medija izaziva posljedice brisanja kako je navedeno u članku 17. stavku 1. OUZP-a. Ako ispitanik zatraži uklanjanje odgovarajućeg računa, voditelj obrade na platformi društvenih medija mora ukloniti podatke. Međutim, platforma društvenih medija smije zadržati neke podatke na određeno vrijeme ako se primjenjuje članak 17. stavak 3. OUZP-a. Iznimke navedene u članku 17. stavku 3. OUZP-a moraju se strogo tumačiti i primjenjive su samo u slučajevima koji su izričito navedeni u tom dijelu odredbe. Voditelj obrade za svaku iznimku na koju se poziva u skladu s člankom 17. stavkom 3. OUZP-a i odgovarajuće zadržavanje podataka mora navesti opravdanje, na primjer ako se nacionalnim pravom propisuje da je voditelj obrade dužan pohraniti

[73] Za razliku od drugih prava ispitanika, vidjeti točku 154.

informacije o ispitaniku zbog prevladavajućih razloga od javnog interesa, radi ostvarivanja temeljnog prava na slobodu izražavanja i informiranja ili zbog poreznih razloga. Podrazumijeva se da bi takve preostale podatke trebao interno pohranjivati samo pružatelj usluga društvenih medija i da ne bi smjeli biti javno dostupni drugim korisnicima. Međutim, izuzeće u skladu s člankom 17. stavkom 3. OUZP-a ni na koji način ne omogućuje pružatelju usluga društvenih medija da održava račun ispitanika dulje nego što su korisnici predvidjeli nakon podnošenja zahtjeva za uklanjanje.

164. Neovisno o zahtjevu za uklanjanje računa, ako korisnici povuku svoju privolu u skladu s člankom 7. stavkom 3. OUZP-a, obrada njihovih podataka danih na temelju privole u skladu s člankom 6. stavkom 1. točkom (a) OUZP-a više se ne može provoditi. U tom se slučaju u određenim okolnostima i dalje mogu provoditi drugi postupci obrade ako se pružatelj usluga društvenih medija oslanja na druge pravne osnove iz članka 6. stavka 1. OUZP-a.

165. Međutim, ako korisnici zatraže uklanjanje svojeg računa, daljnja obrada ne bi se trebala provoditi bez obzira na pravnu osnovu, osim ako se primjenjuje jedna od iznimki navedenih u konačnom popisu u članku 17. stavku 3. OUZP-a. U tom je kontekstu važno imati na umu da je zadržavanje ograničeno na navedenu minimalnu pohranu.

166. U skladu s člankom 25. stavkom 1. OUZP-a voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi načela zaštite podataka proveo u praksi. U skladu sa Smjernicama 4/2019 o članku 25. – Tehnička i integrirana zaštita podataka tehničke i organizacijske mjere mogu se tumačiti u širem smislu kao bilo koja metoda ili način koje voditelj obrade može upotrebljavati pri obradi. Pojam „odgovarajuće" znači da bi te mjere trebale biti prikladne za postizanje predviđene svrhe, odnosno njima se mora provoditi učinkovita zaštita podataka. Zahtjev da mjere budu odgovarajuće stoga je usko povezan sa zahtjevom učinkovitosti[74].

[74] Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka, str. 6, točka 8.

ii. Pauziranje računa

167. Korisnicima se nudi i alternativna mogućnost da privremeno deaktiviraju svoj račun, što im omogućuje da na neko vrijeme napuste društvene medije bez trajnog uklanjanja računa. U tom slučaju račun je privremeno onemogućen, a profil, fotografije, komentari i reakcije bit će skriveni sve dok korisnici ponovno ne aktiviraju svoj račun, npr. ponovnom prijavom. Glavna je razlika u odnosu na brisanje to što osobni podaci ostaju na društvenoj mreži i korisnici mogu ponovno aktivirati račun bez nove registracije.

168. Korisnici koji započnu postupak uklanjanja računa mogu uvidjeti da je umjesto toga unaprijed odabrana opcija pauziranja računa. Iako ponuđena opcija pauziranja može biti korisna za korisnike koji još ne žele trajno ukloniti svoj račun, pružatelji usluga društvenih medija korisnicima ne smiju nametati takva razdoblja mirovanja, posebno kao unaprijed odabranu opciju. Kad pružatelj usluga društvenih medija ponudi mogućnost deaktivacije, korisnici razumno očekuju da se njihovi osobni podaci neće obrađivati jednako kao za vrijeme aktivnog korištenja računa te da će pružatelj usluga društvenih medija u tom razdoblju obrađivati osobne podatke samo ako je to nužno. Korisnici mogu očekivati da se njihovi podaci neće uopće ili u cijelosti obrađivati u određene svrhe, kao što je poboljšanje njihova profila posjećivanjem internetskih stranica trećih strana na kojima se koriste odgovarajući alati za ciljanje ili praćenje. Osim transparentnog informiranja korisnika o posljedicama pauziranja njihova računa, za svaku obradu podataka za vrijeme te pauze mora postojati valjana pravna osnova.

169. Kad je riječ o obradi podataka na temelju privole u skladu s člankom 6. stavkom 1. točkom (a) OUZP-a, pružatelj usluga društvenih medija mora uzeti u obzir da korisnici očekuju da privola koju daju pri registraciji ili nakon nje obuhvaća samo podatke koji se obrađuju za vrijeme njihova aktivnog korištenja računa. EDPB uviđa da trajanje privole ovisi o kontekstu, području primjene prvotne privole i očekivanjima ispitanika[75]. Iako u OUZP-u ne postoji određeni rok trajanja privole, njezina valjanost ovisit će o kontekstu, području primjene izvorne privole i očekivanjima ispitanika[76]. Ako se postupci obrade znatno promijene ili razviju, izvorna privola više nije valjana[77]. EDPB kao najbolju praksu preporučuje da se privola obnavlja u odgovarajućim vremenskim razmacima[78]. Ponovnim dostavljanjem svih informacija osigurava se da ispitanici ostanu dobro informirani o tome kako se upotrebljavaju njihovi podaci i kako mogu ostvariti svoja prava[79]. U tom slučaju potrebno je ponovno ishoditi privolu[80], pri čemu moraju biti ispunjeni svi odgovarajući zahtjevi.

170. Razumna očekivanja ispitanika trebala bi se uzeti u obzir i pri primjeni članka 6. stavka 1. točke (f) OUZP-a (vidjeti uvodnu izjavu 47.). Prije svega nužno je razmotriti može li ispitanik u trenutku i u kontekstu prikupljanja osobnih podataka razumno očekivati da će se obrada provoditi u tu svrhu. Međutim, korisnici razumno očekuju da će se tijekom deaktivacije provoditi samo nužna obrada podataka. Nadalje, pružatelj usluga društvenih medija može se pozvati na legitiman interes samo ako su provedeni svi koraci ispitivanja legitimnog interesa, uključujući odvagivanje. Svaki prevladavajući interes ili temeljna prava i slobode ispitanika trebali bi se procjenjivati za svaki slučaj zasebno.

171. Budući da se za vrijeme deaktivacije u velikoj mjeri suspendiraju i ugovorne obveze, postupci obrade podataka potrebni su samo u ograničenoj mjeri u skladu s člankom 6. stavkom 1. točkom (b) OUZP-a.

[75] Smjernice 5/2020 o privoli, točka 110.
[76] Smjernice 5/2020 o privoli, točka 110.
[77] Smjernice 5/2020 o privoli, točka 110.
[78] Smjernice 5/2020 o privoli, točka 111.
[79] Smjernice 5/2020 o privoli, točka 111.
[80] Vidjeti Smjernice 5/2020 o privoli, točku 110.

Nužnom se može smatrati isključivo pohrana korisničkih podataka do konačne odluke o ponovnoj aktivaciji ili uklanjanju.

172. Budući da je sva prethodna obrada podataka bila usmjerena na aktivan račun, moraju se pružiti dodatne informacije o obradi za vrijeme deaktivacije ako već nisu obuhvaćene općim informacijama u skladu s člancima 13. i 14. OUZP-a. To proizlazi iz načela transparentnosti i poštenosti iz članka 5. stavka 1. točke (a) OUZP-a i ograničavanja svrhe iz članka 5. stavka 1. točke (b) OUZP-a. Ispitaniku se moraju pružiti dostatne informacije o obradi podataka nakon deaktivacije. Pružatelj usluga društvenih medija stoga za vrijeme pauze iscrpno obavješćuje korisnike o stvarnoj obradi i njezinim svrhama te prema potrebi pribavlja novu privolu.

b. Obmanjujući obrasci dizajna

i. Obrasci koji se temelje na sadržaju

Preopterećenost – labirint pravila privatnosti (Prilog I., kontrolni popis 4.1.2.)

173. U ovom scenariju uporabe obmanjujući obrazac dizajna ***labirint pravila privatnosti*** pojavljuje se kad se korisnici obasipaju golemom količinom informacija raspoređenih na više mjesta kako bi ih se odvratilo od uklanjanja računa, kao što je prikazano u sljedećem primjeru. Iako je prije tog koraka prilično poželjno pružiti određene dodatne informacije, na primjer napomenuti da korisnici imaju pristup svojim podacima prije uklanjanja, opće nepovezane informacije više nisu važne. Korisnike ne bi trebalo nepotrebno zadržavati u provedbi tog koraka.

Primjer 52: Korisnik traži pravo na brisanje. Mora otvoriti postavke računa, odabrati podizbornik „Privatnost" i pomaknuti se sve do dna stranice kako bi pronašao poveznicu za uklanjanje računa.

Stimuliranje – upravljanje emocijama (Prilog I., kontrolni popis 4.3.1.)

Primjer 53: Na prvoj razini korisnicima se daju informacije u kojima se ističu samo negativne, obeshrabrujuće posljedice uklanjanja računa (npr. „Izgubit ćeš sve zauvijek" ili „Tvoji prijatelji će te zaboraviti").

174. Iako se iskazivanje žaljenja zbog raskida ugovornog odnosa čini društveno prihvatljivim i stoga ga je teško izraziti u pravnom smislu, navođenje sveobuhvatnog opisa navodnih negativnih posljedica brisanja računa kao u gornjem primjeru, u kojem se pobuđuje strah od propuštanja (FOMO, eng. *fear of missing out*), to je prepreka odluci korisnika jer se stvara dojam da je uklanjanje računa iznimno nezahvalan postupak. Takvim ***upravljanjem emocijama*** korisnika uz prijetnju da će ostati sami ako uklone svoj račun krši se obveza olakšavanja ostvarivanja prava ispitanika iz članka 12. stavka 2. OUZP-a, kao i načelo poštenosti iz članka 5. stavka 1. točke (a) OUZP-a.

Držanje u neznanju – dvosmisleni tekst ili informacije (Prilog I., kontrolni popis 4.6.3.)

175. U kontekstu uklanjanja računa na društvenim medijima korisnici mogu naići i na obmanjujući obrazac dizajna ***dvosmisleni tekst ili informacije***, kako je prikazano u sljedećem primjeru.

Primjer 54: Kad korisnik ukloni svoj račun, ne dobiva obavijest o tome koliko će se dugo njegovi podaci čuvati nakon uklanjanja računa. Što je još gore, korisniku se ni u jednom trenutku u cijelom postupku uklanjanja ne napominje da se „neki osobni podaci" mogu

pohraniti čak i nakon uklanjanja računa. Mora sam tražiti informacije iz dostupnih izvora informacija.

Primjer 55: Korisnici mogu ukloniti svoj račun samo klikom na poveznice s tekstom „Vidimo se" ili „Deaktivacija" dostupnih na njihovu računu.

176. U tim primjerima tekst poveznica sročen je tako da nije jasno da će korisnici biti preusmjereni na postupak uklanjanja računa. Korisnici će umjesto toga vjerojatno pretpostaviti da je riječ o drugim funkcijama, kao što su odjava do sljedećeg korištenja ili deaktivacija računa. To bi se moglo tumačiti kao povreda članka 12. stavka 2. OUZP-a, u kojem se navodi da bi voditelji obrade trebali olakšati ostvarivanje prava ispitanika. Budući da korisnicima nije jasno što očekivati u vezi s poveznicom, platforma društvenih medija ne olakšava u potpunosti ostvarivanje prava na brisanje. Korištenjem takvih dvosmislenih riječi u drugom kontekstu mogle bi se prekršiti odredbe OUZP-a kao što je članak 7., a time i članak 17. stavak 1. točka (b).

ii. Obrasci koji se temelje na sučelju

Preskakanje – obmanjujući komfor (Prilog I., kontrolni popis 4.2.1.)

Primjer 56: U postupku uklanjanja računa korisnicima se nude dvije opcije: uklanjanje ili pauziranje računa. Prema zadanim postavkama odabrana je opcija pauziranja.

177. Prvom opcijom, koja se odnosi na uklanjanje računa, uklanjaju se svi osobni podaci korisnika, što znači da platforma društvenih medija više ne posjeduje te podatke, osim podataka na temelju privremene iznimke iz članka 17. stavka 3. OUZP-a. S druge strane, ako se odabere druga opcija, pauziranje računa, pružatelj usluga društvenih medija čuva i potencijalno obrađuje sve osobne podatke. To je nužno veći rizik za ispitanika, na primjer ako dođe do povrede podataka i ako se pristupa podacima koje pružatelj usluga društvenih medija i dalje pohranjuje te ako se oni umnožavaju, prenose ili drukčije obrađuju. Zadani izbor opcije pauziranja vjerojatno će potaknuti korisnike da se odluče za nju umjesto da uklone svoj račun kako su prvotno namjeravali. Praksa opisana u ovom primjeru stoga se može smatrati povredom članka 12. stavka 2. OUZP-a jer se u ovom slučaju ne olakšava ostvarivanje prava na brisanje, nego se čak i pokušava odvratiti korisnike od njegova ostvarivanja.

Preskakanje – odvraćanje pozornosti (Prilog I., kontrolni popis 4.2.2.)

178. Pružanje mogućnosti da korisnici preuzmu svoje podatke kad izraze želju da uklone svoj račun može biti važna opcija. Naime, kad se njihov račun ukloni, njihovi osobni podaci bit će izbrisani nakon određenog razdoblja. To znači da će u cijelosti izgubiti svoje osobne podatke ako ne dobiju njihovu kopiju. Međutim, način prikazivanja te mogućnosti može slijediti obmanjujući obrazac dizajna poznat kao ***odvraćanje pozornosti***, kao što je prikazano u sljedećem primjeru.

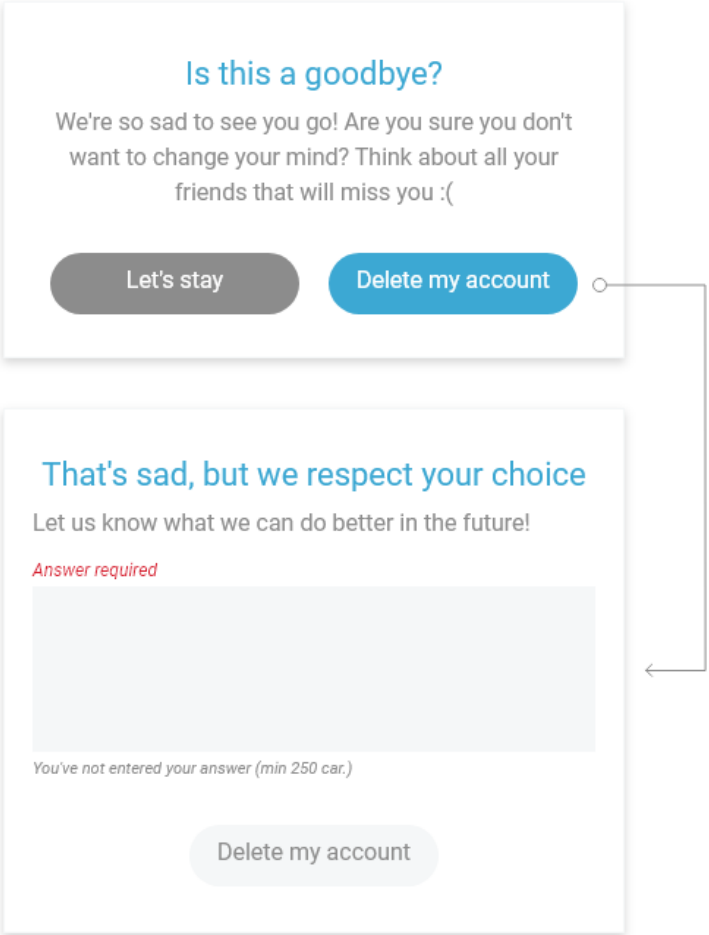
Primjer 57: Nakon što korisnik klikne na opciju „Ukloni moj račun", nudi mu se mogućnost da prije uklanjanja račun preuzme svoje podatke, kojom se provodi pravo na prenosivost. Kad klikne na opciju za preuzimanje podataka, korisnik se preusmjerava na stranicu s informacijama o preuzimanju. Međutim, nakon što korisnik odabere podatke koje želi preuzeti i način njihova preuzimanja, ne preusmjerava ga se na postupak uklanjanja.

179. U prethodnom primjeru može se zaključiti da način provedbe opcije preuzimanja ne olakšava ostvarivanje prava na brisanje povezanog s uklanjanjem računa. Naime, nakon što korisnik preuzme

svoje podatke, ne vraća ga se na postupak uklanjanja. Morat će kliknuti više puta da bi se vratio. Takvim ometanjem ostvarivanja prava krši se članak 12. stavak 2. OUZP-a. Nadalje, značajku za jednostavan pristup postupku brisanja nakon preuzimanja podataka jednostavno je uvesti. U tom bi se smislu moglo smatrati da se ne poštuje obveza provedbe odgovarajućih tehničkih i organizacijskih mjera iz članka 25. stavka 1. OUZP-a jer korisnici ne mogu nastaviti s učinkovitim ostvarivanjem svojih prava.

Ometanje – dulje trajanje od nužnog (Prilog I., kontrolni popis 4.4.2.)

180. Kao što je detaljno opisano u scenariju uporabe 4, svi nerelevantni koraci u ostvarivanju prava mogli bi biti u suprotnosti s odredbama OUZP-a, posebno s člankom 12. stavkom 2. To se odnosi na trenutak u kojem korisnici žele ukloniti svoj račun jer bi se time zadiralo u pravo na brisanje povezano s takvim zahtjevom.



Primjer 58: U ovom primjeru korisnik prvo vidi potvrdni okvir za brisanje svojeg računa nakon što klikne na odgovarajuću poveznicu ili gumb na svojem računu. Iako taj okvir sadržava određene elemente ***upravljanja emocijama***, taj se korak može smatrati sigurnosnom mjerom kako korisnici ne bi uklonili svoj račun zbog pogrešnog klika na svojem računu. Međutim, kad korisnik klikne na gumb „Ukloni moj račun", prikazuje mu se drugi okvir u kojem se od njega traži da opiše zašto želi napustiti račun. Korisnik ne može ukloniti račun sve dok ne unese tekst u taj okvir jer je gumb povezan s tom radnjom neaktivan i sive boje. Zbog opisane

prakse brisanje računa traje ***dulje nego što je nužno***, posebno zato što korisnik mora uložiti dodatan trud i vrijeme kako bi udovoljio zahtjevu i opisao zašto želi napustiti račun, a to ne bi trebao biti preduvjet za uklanjanje računa.

181. Kao što je prethodno navedeno, pri ostvarivanju određenog prava korisnike ne bi trebalo primoravati da odgovaraju na pitanja koja nisu povezana s ostvarivanjem tog prava. Obveza obrazlaganja svojeg izbora ili objašnjavanja kako bi trebalo poboljšati platformu društvenih medija nije obuhvaćena tom kategorijom. U opisanom primjeru to je pitanje posebno problematično jer ispitanici moraju napisati odgovor umjesto da odaberu unaprijed sastavljeni prijedlog na popisu, što ih još više opterećuje jer moraju sami osmisliti cijeli odgovor. Takav bi mehanizam korisnicima kojima nije ugodno unositi odgovor mogao posve uskratiti mogućnost ostvarivanja prava.

182. Međutim, to ne znači da je popis unaprijed sastavljenih odgovora prihvatljiv korak koji treba uvrstiti u postupak uklanjanja računa, posebno ako su ti odgovori povezani s daljnjim koracima i radnjama koji se nameću korisnicima, kao što pokazuje primjer u nastavku.

Primjer 59: Pružatelj usluga društvenih medija obvezuje korisnike da odgovore na pitanje o razlozima zbog kojih žele izbrisati svoj račun odabirom odgovora iz padajućeg izbornika. Korisnici smatraju da će, ako odgovore na to pitanje, moći izvršiti željenu radnju, odnosno ukloniti račun. Nakon odabira odgovora pojavljuje se skočni prozor u kojem se prikazuju rješenja problema navedenog u njihovu odgovoru. Dakle, odgovaranje na pitanje usporava postupak brisanja računa korisnika.

183. Osim što znatno produljuje brisanje računa, mehanizam ***odvraćanja pozornosti*** nastoji odvratiti korisnike od uklanjanja njihova računa predlaganjem rješenja za njihov razlog napuštanja platforme društvenih medija. Tako se ometa ostvarivanje prava na brisanje, a samim time i odvraća ispitanike od ostvarivanja njihova prava.

Nestalnost – dekontekstualizacija (Prilog I., kontrolni popis 4.5.2.)

184. Naposljetku, pri pokušaju korisnika da ukloni svoj račun može se pojaviti i obmanjujući obrazac dizajna poznat kao ***dekontekstualizacija***.

Primjer 60: Na platformi društvenih medija XY poveznica za deaktivaciju ili uklanjanje računa nalazi se u kartici „Vaši podaci na platformi XY".

185. Općenito, pojmovi u naslovu stranice ili odjeljka platforme društvenih medija posvećenog pitanjima zaštite podataka trebali bi jasno upućivati na vrstu informacija ili kontrole koje su ondje dostupne. Prosječni korisnici vjerojatno neće povezati radnje za uklanjanje ili deaktivaciju svojeg računa s upravljanjem podacima. U prethodnom primjeru korisnici ne bi očekivali da će se funkcija uklanjanja računa nalaziti na stranici pod nazivom „Vaše informacije na platformi XY", koji implicira da se na stranici prikazuju i potencijalno pregledavaju osobne informacije. Umjesto toga, tražili bi stranicu „Općenito" ili „Izbriši moj račun". Stoga su sa stajališta korisnika te opcije smještene u postavku koja je izvan konteksta i ne odgovara očekivanjima korisnika.

Primjer 61: Stvarna kartica za brisanje računa nalazi se u odjeljku „Uklonite funkciju svojeg računa".

186. U ovom primjeru korisnici bi mogli pogrešno shvatiti naslov odjeljka i pretpostaviti da je riječ o mjestu gdje samo mogu prilagoditi pojedinačne funkcije. Korisnici stoga ne bi očekivali da postoji mogućnost uklanjanja cijelog računa. To korisnicima otežava pronalaženje odgovarajuće poveznice za brisanje cijelog računa.

187. Obmanjujući obrazac dizajna ***dekontekstualizacija***, kako je opisan u dvama prethodnim primjerima, mogao bi se smatrati povredom članka 12. stavka 2. OUZP-a s obzirom na to da bi korisnici imali poteškoća u pronalaženju odgovarajućeg mjesta za ostvarivanje prava na brisanje.

c. Primjeri dobre prakse

Usklađeni tekst: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Navođenje definicija: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Korištenje primjera: vidjeti definiciju u scenariju uporabe 1 (str. 22).

Objašnjavanje posljedica: vidjeti definiciju u scenariju uporabe 2c (str. 32).

Dosljednost na različitim uređajima: vidjeti definiciju u scenariju uporabe 3a (str. 39).

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

4. PRILOG I.: POPIS KATEGORIJA I VRSTA OBMANJUJUĆIH OBRAZACA DIZAJNA

Sljedeći popis sadržava pregled kategorija obmanjujućih obrazaca dizajna i vrsta unutar svake kategorije. U njemu se navode i odredbe OUZP-a koje su najrelevantnije za vrste obmanjujućih obrazaca dizajna. Čitatelji bi trebali imati na umu da je, kako je prethodno navedeno, načelo poštene obrade utvrđeno u članku 5. stavku 1. točki (a) OUZP-a polazište za procjenu prisutnosti obmanjujućih obrazaca dizajna. Ono ima krovnu funkciju i nijedan obmanjujući obrazac dizajna ne bi bio u skladu s njim neovisno o tome je li usklađen s drugim načelima zaštite podataka[81].

U popisu se navode i brojevi primjera i odgovarajući scenarij uporabe (SU) za svaki obrazac kako bi ih čitatelji brzo pronašli.

Važno je napomenuti da ovaj popis nije potpun i da se obmanjujući obrasci dizajna mogu pojaviti i u scenarijima uporabe za koje u tekstu Smjernica nije naveden primjer pojedine vrste obmanjujućeg obrasca dizajna.

4.1. Preopterećenost

Obasipanje korisnika golemom količinom zahtjeva, informacija, opcija ili mogućnosti kako bi ih se odvratilo od određenog postupka i navelo da zadrže ili prihvate određenu praksu povezanu s podacima.

4.1.1. Kontinuirano prikazivanje upita[82]

Poticanje korisnika da daju više osobnih podataka nego što je nužno za svrhu obrade ili da pristanu na drukčije korištenje svojih podataka opetovanim prikazivanjem zahtjeva u kojima se od njih traži da daju podatke ili da pristanu na novu svrhu obrade. Takvi opetovani upiti mogu se prikazivati na jednom ili više uređaja. Korisnici će vjerojatno popustiti jer ih odbijanje zahtjeva pri svakom korištenju platforme iscrpljuje i ometa im korištenje.

Relevantne odredbe OUZP-a:

- *ograničavanje svrhe: članak 5. stavak 1. točka (b)*
- *dobrovoljna privola: članak 7.* u vezi s člankom 4. točkom 11.
- *posebna privola: članak 7. stavak 2.*

Primjeri: SU 1, primjeri 1, 2; SU 3a, primjer 34 (ilustracija).

4.1.2. Labirint pravila privatnosti

Kad korisnici žele dobiti određene informacije ili primijeniti posebnu kontrolu odnosno ostvariti pravo ispitanika, posebno im je teško pronaći te značajke jer moraju otvarati prevelik broj stranica kako bi došli do relevantne informacije ili kontrole, a nije im dostupan sveobuhvatan i iscrpan pregled. Korisnici će vjerojatno odustati ili previdjeti relevantne informacije ili kontrolu.

[81] Vidjeti točku 9. ovih Smjernica.

[82] Taj je obrazac blisko povezan s vrstom obrasca koji se u akademskoj literaturi naziva „dosađivanje" (eng. *nagging*).

Relevantne odredbe OUZP-a:

- *načelo transparentnosti: članak 5. stavak 1. točka (a) i transparentne informacije: članak 12. stavak 1.*
- *načelo poštenosti: članak 5. stavak 1. točka (a)*
- *lako dostupne informacije*: članak 12. stavak 1.
- *jednostavan pristup pravima*: članak 12. stavak 2.
- *informirana privola:* članak 7. u vezi s člankom 4. točkom 11.

Primjeri: SU 2a, primjer 17; SU 3a, primjer 33; SU 3b, primjer 37; SU 4, primjeri 47 (ilustracija) i 48 (ilustracija); SU 5, primjer 51.

4.1.3. Previše opcija

Izlaganje korisnika (pre)velikom broju opcija za odabir. Zbog previše opcija za odabir korisnici ne mogu donijeti odluku ili im određene postavke promaknu, posebno ako nisu dostupne informacije. Zbog toga naposljetku mogu odustati ili zanemariti postavke svojih preferencija ili prava povezanih za zaštitom podataka.

Relevantne odredbe OUZP-a:

- *načela transparentnosti i poštenosti:* članak 5. stavak 1. točka (a)
- *transparentne informacije:* članak 12. stavak 1.

Primjer: SU 3b, primjer 35.

4.2. Preskakanje

Dizajniranje sučelja ili korisničkog putovanja tako da korisnici zaborave ili ne razmišljaju o svim ili nekim aspektima zaštite podataka.

4.2.1. Obmanjujući komfor

Prema zadanim postavkama omogućene su značajke i opcije najinvazivnije za podatke. Zbog učinka zadanih postavki koji potiče pojedince da zadrže unaprijed odabranu opciju nije vjerojatno da će je korisnici promijeniti čak i ako im se za to pruži mogućnost.

Relevantne odredbe OUZP-a:

- *tehnička i integrirana zaštita podataka:* članak 25. stavak 1.
- *privola:* članak 4. točka 11. i članak 6. (nezakonita praksa aktivacije obrade na temelju automatski zadane privole).

Primjeri: SU 1, primjer 9; SU 3b, primjeri 39 i 40 (ilustracija); SU 5, primjer 55.

4.2.2. Odvraćanje pozornosti

Radnja ili informacije povezane sa zaštitom podataka nude se istodobno s drugim elementom koji može ili ne mora biti povezan sa zaštitom podataka. Ako korisnici odaberu tu drugu opciju koja im je odvratila pozornost, vjerojatno će zaboraviti na opciju povezanu sa zaštitom podataka, čak i ako su na nju prvotno bili usredotočeni.

Relevantne odredbe OUZP-a:

- *načela transparentnosti i poštenosti:* članak 5. stavak 1. točka (a)
- *transparentne informacije:* članak 12. stavak 1.
- *ostvarivanje prava:* članak 12. stavak 2.

Primjeri: SU 2c, primjer 25; SU 3a, primjer 29; SU 5, primjeri 56 i 58.

4.3. Stimuliranje

Vršenje utjecaja na izbor korisnika pobuđivanjem emocija ili vizualnim poticajima.

4.3.1. Upravljanje emocijama[83]

Korištenje teksta ili vizualnih elemenata (stil, boje, slike ili drugo) kako bi se korisnicima predstavile informacije na vrlo pozitivan način, zbog čega se oni osjećaju dobro, sigurno ili nagrađeno, ili na vrlo negativan, zbog čega se osjećaju uplašeno, krivo ili kažnjeno. Takav utjecaj na emocionalno stanje korisnika vjerojatno će ih potaknuti da postupe protivno svojim interesima u području zaštite podataka.

Relevantne odredbe OUZP-a:

- *načela transparentnosti i poštenosti:* članak 5. stavak 1. točka (a)
- *transparentne informacije:* članak 12. stavak 1.
- *ostvarivanje prava:* članak 12. stavak 2.
- *privola djeteta:* članak 8.
- *informirana privola:* članak 7. u vezi s člankom 4. točkom 11.

Primjeri: SU 1, primjeri 4, 5, 6; SU 5, primjer 52.

4.3.2. Skrivanje na vidljivom mjestu

Korištenje vizualnog stila ili tehnike za informacije ili kontrole zaštite podataka kojima se korisnike usmjerava prema manje restriktivnim, a time i invazivnijim opcijama.

Relevantne odredbe OUZP-a:

[83] Taj je uzorak blisko povezan s vrstom uzorka koji se naziva „poigravanje s emocijama" (eng. *Toying with Emotions*) i koji se među ostalim spominje u izvješćima međuvladinih organizacija kao što je Europska komisija, Glavna uprava za pravosuđe i zaštitu potrošača, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., i dr., *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report*, Ured za publikacije Europske unije, 2022., https://data.europa.eu/doi/10.2838/859030 i OECD (2022.), „Dark commercial patterns", *Documents de travail de l'OCDE sur l'économie numérique*, n° 336, Éditions OCDE, Pariz, https://doi.org/10.1787/44f5e846-en.

- *načelo poštenosti*: članak 5. stavak 1. točka (a)
- *dobrovoljna privola:* članak 7. u vezi s člankom 4. točkom 11.
- *jasne informacije*: članak 12. stavak 1.
- *ostvarivanje prava:* članak 12. stavak 2.

Primjeri: SU 1, primjer 8, SU 3a, primjer 34 (ilustracija); SU 3b, primjer 40 (ilustracija); SU 4, primjer 48.

4.4. Ometanje[84]

Sprečavanje ili blokiranje korisnika u postupku dobivanja informacija ili upravljanja njihovim podacima otežavanjem ili onemogućavanjem tog koraka.

4.4.1. Slijepa ulica

Kad korisnici traže određene informacije ili kontrolu, ne uspijevaju ih pronaći jer poveznica za preusmjeravanje ne funkcionira ili uopće nije dostupna. Korisnici ne mogu dovršiti tu radnju.

Relevantne odredbe OUZP-a:

- *lako dostupne informacije*: članak 12. stavak 1.
- *ostvarivanje prava*: članak 12. stavak 2.
- *tehnička i integrirana zaštita podataka:* članak 25. stavak 1.

Primjeri: SU 1, primjeri 10, 11; SU 2a, primjer 18; SU 3a, primjeri 30, 31; SU 4, primjer 43.

4.4.2. Dulje trajanje od nužnog

Kad korisnici pokušaju aktivirati kontrolu povezanu sa zaštitom podataka, korisničko putovanje osmišljeno je tako da je za tu aktivaciju potrebno poduzeti više koraka nego za aktivaciju opcija invazivnih za podatke. To će ih vjerojatno odvratiti od aktiviranja takve kontrole.

Relevantne odredbe OUZP-a:

- *lako dostupne informacije*: članak 12. stavak 1.
- *ostvarivanje prava*: članak 12. stavak 2.
- *pravo na prigovor:* članak 21. stavak 1.
- *povlačenje suglasnosti*: članak 7. stavak 3.
- *tehnička (i integrirana) zaštita podataka:* članak 25. stavak 1.

Primjeri: SU 1, primjer 7; SU 3a, primjer 32; SU 4, primjer 50; SU 5, primjeri 57 (ilustracija) i 58.

[84] Ova kategorija blisko je povezana sa strategijom pod nazivom *obstruction* (zapreka), definiranom i opisanom u Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph i Toombs Austin L. 2018. „The Dark (Patterns) Side of UX Design". U *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Kanada) (CHI '18). ACM, New York, NY, SAD, članak 534., 14 stranica. https://doi.org/10.1145/3173574.3174108.

4.4.3. Zavaravajuća radnja

Nepodudarnost između informacija i raspoloživih radnji potiče korisnike da učine nešto što ne namjeravaju. Budući da je ono što korisnici dobiju različito od onog što očekuju, vjerojatno će odustati od daljnjih koraka.

Relevantne odredbe OUZP-a:

- *transparentne informacije:* članak 12. stavak 1.
- *poštenost obrade:* članak 5. stavak 1. točka (a)
- *informirana privola:* članak 7. stavak 2. u vezi s člankom 4. točkom 11.

Primjeri: SU 1, primjer 3; SU 3a, primjer 28.

4.5. Nestalnost

Dizajn sučelja nestabilan je i nedosljedan, što korisnicima otežava da shvate prirodu obrade, pravilno odaberu postavke svojih podataka i otkriju gdje se nalaze kontrole.

4.5.1. Nedostatak hijerarhije

Informacije povezane sa zaštitom podataka nemaju hijerarhiju, zbog čega se pojavljuju više puta i prikazuju na više načina. Korisnike će taj višak informacija vjerojatno zbuniti i neće moći u potpunosti shvatiti kako se njihovi podaci obrađuju i kako ih nadzirati.

Relevantne odredbe OUZP-a:

- *lako dostupne informacije*: članak 12. stavak 1.
- *ostvarivanje prava: članak 12. stavak 2.*

Primjeri: SU 2a, primjeri 13. i 14.

4.5.2. Dekontekstualizacija

Informacija ili kontrola povezana sa zaštitom podataka nalazi se na stranici koja je izvan konteksta. Korisnici vjerojatno neće pronaći tu informaciju ili kontrolu jer ne bi bilo intuitivno tražiti ih na toj stranici.

Relevantne odredbe OUZP-a:

- *lako dostupne informacije*: članak 12. stavak 1.
- *transparentne informacije:* članak 12. stavak 1.
- *ostvarivanje prava: članak 12. stavak 2.*

Primjeri: SU 3b, primjeri 41, 42; SU 5, primjeri 59 i 60.

4.5.3. Nedosljedno sučelje

Sučelje nije dosljedno u različitim kontekstima (npr. u izborniku povezanom sa zaštitom podataka na mobilnom telefonu i računalu ne prikazuju se iste stavke) ili ne odgovara

očekivanjima korisnika (npr. lokacija jedne opcije zamijenjena je lokacijom druge opcije). Zbog tih razlika korisnici možda neće pronaći željenu kontrolu ili informacije ili će koristiti elemente sučelja iz navike, iako ta interakcija dovodi do neželjenog izbora u smislu zaštite podataka.

Relevantne odredbe OUZP-a:

- *lako dostupne informacije*: članak 12. stavak 1.
- *ostvarivanje prava: članak 12. stavak 2.*

Primjeri: SU 3b, primjer 39; SU 4, primjer 50.

4.5.4. Jezični diskontinuitet

Informacije povezane sa zaštitom podataka nisu dostupne na nekom od službenih jezika zemlje u kojoj korisnici žive, iako se sama usluga pruža na tom jezicku. Ako korisnici ne vladaju jezikom na kojem su dostupne informacije o zaštiti podataka, neće ih moći lako pročitati i stoga vjerojatno neće znati kako se podaci obrađuju.

Relevantne odredbe OUZP-a:

- *poštenost obrade:* članak 5. stavak 1. točka (a)
- *razumljive informacije:* članak 12. stavak 1., članak 13. i članak 14.
- *uporaba jasnog i jednostavnog jezika za informacije*: članak 12. stavak 1., članak 13. i članak 14.

Primjeri: SU 2a, primjer 16; SU 3a, primjeri 26 (ilustracija) i 27; SU 4, primjer 44.

4.6. Držanje u neznanju

Sučelje je dizajnirano tako da se prikriju informacije ili kontrole povezane sa zaštitom podataka ili da korisnici nisu sigurni kako se podaci obrađuju i kako ih mogu nadzirati.

4.6.1. Proturječne informacije

Korisnicima se pružaju informacije koje su na neki način međusobno proturječne. Korisnici vjerojatno neće biti sigurni što bi trebali učiniti i koje su posljedice njihovih postupaka, tako da vjerojatno neće poduzeti ništa, nego će samo zadržati zadane postavke.

Relevantne odredbe OUZP-a:

- *poštenost obrade:* članak 5. stavak 1. točka (a)
- *transparentne informacije:* članak 12. stavak 1.
- *informirana privola:* članak 7. stavak 2. u vezi s člankom 4. točkom 11.

Primjeri: SU 2a, primjer 12; SU 2c, primjer 20; SU 3b, primjer 36.

4.6.2. Dvosmisleni tekst ili informacije

Korištenje dvosmislenih i nejasnih pojmova pri pružanju informacija korisnicima. Korisnici vjerojatno neće biti sigurni kako će se podaci obrađivati ili kako mogu nadzirati svoje osobne podatke.

Relevantne odredbe OUZP-a:

- *poštenost obrade:* članak 5. stavak 1. točka (a)
- *transparentne informacije:* članak 12. stavak 1.
- *uporaba jasnog i jednostavnog jezika za informacije*: članak 12. stavak 1.
- *informirana privola:* članak 7. stavak 2. u vezi s člankom 4. točkom 11.
- *nepotpune informacije:* članak 13.
- *posebne odredbe ovisno o konkretnom scenariju uporabe, na primjer članak 34. za SU 2c.*

Primjeri: SU 2a, primjer 15; SU 2c, primjeri 21, 22, 23, 24; SU 4, primjer 45; SU 5, primjeri 53 i 54.

LIFECYCLE
DECEPTIVE DESIGN OVERVIEW
GDPR PROVISIONS
All deceptive design go against the fairness principle
UC 1. Creating an account
UC2. Getting informed
UC3. Staying protected
UC4. Exercising one's right
UC5. Closing / Pausing the account
Purpose limitation
Data protection by design and default
Transparency/Information
Consent
Exercise of the rights
OVERLOADING
Continuous Prompting
Privacy Maze
Too Many Options
SKIPPING
Deceptive Snugness
Look Over There
STIRRING
Emotional Steering
Hidden in Plain Sight
OBSTRUCTING
Dead End
Longer Than Necessary
Misleading Action
FICKLE
Lacking Hierarchy
Decontextualising
Inconsistent Interface
Language Discontinuity
LEFT IN THE DARK
Conflicting Information
Ambiguous Wording or Information

5. PRILOG II.: PRIMJERI DOBRE PRAKSE

U sljedećem popisu daje se pregled primjera dobre prakse navedenih u Smjernicama na kraju svakog scenarija uporabe. Oni se mogu uzeti u obzir pri dizajniranju korisničkih sučelja koja olakšavaju djelotvornu provedbu OUZP-a. Ti primjeri dobre prakse mogu biti prvi korak prema standardiziranom postupku kojim će korisnici učinkovito nadzirati svoje podatke i ostvarivati svoja prava.

Prečaci: poveznice na informacije, radnje ili postavke koje korisnicima mogu olakšati upravljanje njihovim podacima i postavkama zaštite podataka trebale bi biti dostupne svaki put kad korisnici naiđu na povezane informacije ili iskustvo (*npr. poveznice na relevantne dijelove pravila zaštite privatnosti*; *npr. u pravilima zaštite privatnosti za svaku informaciju o zaštiti podataka navedite poveznice koje vode izravno na povezane stranice o zaštiti podataka na platformi društvenih medija; korisnicima osigurajte poveznicu za ponovno postavljanje lozinke*; *kad se korisnici obavještavaju o određenom aspektu obrade, poziva ih se da postave vlastite preferencije podataka na odgovarajućoj stranici s postavkama / nadzornoj ploči; osigurajte poveznicu na opciju uklanjanja računa u korisničkom računu).*

Skupne opcije: grupiranje opcija koje imaju istu svrhu obrade kako bi ih korisnici lakše mijenjali, pri čemu i dalje mogu unositi granularne izmjene. Ako platforme društvenih medija nude skupne opcije, one ne bi smjele sadržavati neočekivane ili nepovezane elemente (npr. elementi s različitom svrhom). Ako je za obradu potrebna privola, skupne opcije moraju biti u skladu sa Smjernicama EDPB-a o privoli, posebno točkama od 42. do 44.

Podaci za kontakt: u pravilima zaštite privatnosti trebala bi biti jasno navedena adresa poduzeća za slanje zahtjeva povezanih sa zaštitom podataka. Trebala bi se nalaziti u odjeljku u kojem je korisnici mogu očekivati, kao što je odjeljak o identitetu voditelja obrade, odjeljak o pravima ili odjeljak s podacima za kontakt.

Obraćanje nadzornom tijelu: konkretno imenovanje nadzornog tijela uz poveznicu na njegove internetske stranice ili posebne internetske stranice za podnošenje prigovora. Te bi informacije trebale biti navedene u odjeljku u kojem ih korisnici mogu očekivati, kao što je odjeljak o pravima.

Pregled pravila zaštite privatnosti: na početku/vrhu pravila zaštite privatnosti treba navesti sadržaj s naslovima i podnaslovima (koji se može sakriti i prikazati po želji) s prikazom odlomaka iz obavijesti o zaštiti privatnosti. Nazivi pojedinih odlomaka jasno usmjeravaju korisnike na konkretni sadržaj i omogućuju im da brzo uoče i otvore odjeljak koji traže.

Praćenje promjena i usporedba: ako se u obavijest o zaštiti privatnosti unesu izmjene, trebaju biti dostupne prethodne verzije s datumom objave i istaknutim izmjenama.

Usklađeni tekst: na internetskim stranicama koristi se isti tekst i definicija za istu vrstu zaštite podataka. Tekst naveden u pravilima zaštite privatnosti trebao bi odgovarati tekstu na ostatku platforme.

Navođenje definicija: kad koristite nepoznate ili tehničke riječi ili izraze, navođenje definicije jednostavnim jezikom pomoći će korisnicima da razumiju pružene informacije. Definicija se može staviti u sam tekst, pojaviti se kad korisnici prijeđu pokazivačem miša iznad odgovarajuće riječi ili biti navedena u pojmovniku.

Isticanje elemenata zaštite podataka: vizualno upečatljiv prikaz elemenata ili radnji povezanih sa zaštitom podataka na sučelju koje nije izravno posvećeno predmetnoj temi. Na primjer, pri dijeljenju javnog sadržaja na platformi kontrole za povezivanje geolokacije trebale bi biti izravno dostupne i jasno vidljive.

Uvod u zaštitu podataka: odmah nakon izrade računa pružatelj usluga društvenih medija treba u uvodnu fazu njihova korištenja uvrstiti elemente zaštite podataka kako bi korisnicima omogućio da bez teškoća prouče i prilagode svoje preferencije. Na primjer, može ih se pozvati da prilagode svoje preferencije zaštite podataka nakon što dodaju prvog prijatelja ili podijele prvu objavu.

Korištenje primjera: osim obveznih informacija u kojima se jasno i precizno navodi svrha obrade, određena vrsta obrade podataka može se ilustrirati primjerima kako bi je korisnici lakše razumjeli.

Fiksna navigacija (eng. *sticky navigation*): za vrijeme pregledavanja stranice koja se odnosi na zaštitu podataka sadržaj se može stalno prikazivati na zaslonu, tako da se korisnici uvijek mogu snaći na stranici i brzo prolaziti sadržajem zahvaljujući usidrenim poveznicama.

Povratak na vrh: postavite gumb za povratak na vrh na dno stranice ili kao fiksni element na dnu prozora da biste korisnicima olakšali navigaciju na stranici.

Obavijesti: obavijesti mogu korisnike informirati o aspektima, promjenama ili rizicima povezanima s obradom osobnih podataka (*npr. kad je došlo do povrede podataka*). Te obavijesti mogu se dostavljati u više oblika, kao što su poruke u ulaznom spremniku računa, skočni prozori ili fiksne obavijesti na vrhu internetske stranice.

Objašnjavanje posljedica: ako korisnici žele aktivirati ili deaktivirati kontrolu zaštite podataka ili dati ili povući privolu, obavijestite ih o posljedicama te radnje neutralnim tonom.

Dosljednost na različitim uređajima: ako je platforma društvenih medija dostupna na različitim uređajima (npr. računalo, pametni telefoni), postavke i informacije povezane sa zaštitom podataka trebale bi se nalaziti na istim mjestima u različitim verzijama i obuhvaćati iste korake i elemente sučelja (izbornik, ikone itd.).

Registar zaštite podataka: radi lakšeg snalaženja u različitim dijelovima izbornika korisnicima stavite na raspolaganje lako dostupnu stranicu na kojoj će moći pristupiti svim radnjama i informacijama povezanima sa zaštitom podataka. Ta stranica može se nalaziti u glavnom navigacijskom izborniku pružatelja usluga društvenih medija, korisničkom računu, pravilima zaštite privatnosti itd.

Kontekstualne informacije: osim iscrpnih pravila zaštite privatnosti treba navesti kratke informacije u najprikladnijem trenutku kako bi korisnik raspolagao konkretnim i stalnim informacijama o načinu obrade njegovih podataka.

URL koji je razumljiv sam po sebi: za stranice koje se odnose na postavke ili informacije povezane sa zaštitom podataka trebalo bi koristiti internetsku adresu koja jasno odražava njihov sadržaj. Na primjer, za stranicu na kojoj je centraliziran nadzor zaštite podataka može se koristiti URL kao što je [social-network.com]/data-settings.

Obrazac za ostvarivanje prava: da biste korisnicima olakšali ostvarivanje njihovih prava iz OUZP-a, ponudite poseban obrazac koji će im pomoći da razumiju svoja prava i voditi ih u podnošenju takvih zahtjeva.