

Bruxelles, 12.9.2018.
COM(2018) 638 final

Slobodni i poštteni izbori

SMJERNICE

Smjernice Komisije o primjeni prava Unije o zaštiti podataka u kontekstu izbora

*Doprinos Europske komisije sastanku čelnika u
Salzburgu 19.-20.rujna 2018.*

SMJERNICE KOMISIJE O PRIMJENI PRAVA UNIJE O ZAŠTITI PODATAKA U KONTEKSTU IZBORA

Suradnja s biračima temelj je demokratskog procesa. Političke stranke trajno moraju prilagođavati komunikaciju u kontekstu izbora svojoj publici i uzimati u obzir njezine posebne interese. Stoga je prirodno da akteri koji sudjeluju u izborima proučavaju mogućnosti uporabe podataka za dobivanje glasova. Razvojem digitalnih alata i internetskih platformi nastale su mnoge nove prilike za sudjelovanje u političkim raspravama s građanima.

Razvoj tehnika za mikrociljanje na temelju nezakonite obrade osobnih podataka, primjerice u slučaju poduzeća Cambridge Analytica, primjer je druge vrste procesa. Taj primjer oslikava pitanja koja nastaju zbog modernih tehnologija, ali ukazuje i na osobitu važnost zaštite podataka u kontekstu izbora. To je postalo ključno pitanje ne samo za pojedince nego i za funkcioniranje naših demokracija jer je riječ o ozbiljnoj prijetnji pravednom i demokratskom procesu izbora koja može ugroziti otvorenu raspravu, pravednost i transparentnost – ključne čimbenike demokracije. Komisija smatra da je rješavanje tog problema od ključne važnosti kako bi se vratilo povjerenje javnosti u pravednost izbornog procesa.

Prva izvješća Ureda povjerenika za informiranje (tijela Ujedinjene Kraljevine za zaštitu podataka) o uporabi analize podataka u političkim kampanjama¹ i mišljenje Europskog nadzornika za zaštitu podataka o manipulaciji na internetu i osobnim podacima² potvrđuju sve veći učinak mikrociljanja u komercijalne svrhe u kontekstu izbora.

Općenito, nekoliko tijela za zaštitu podataka dalo je mišljenje o zaštiti podataka u kontekstu izbora³.

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća (Opća uredba o zaštiti podataka)⁴, koja je postala izravno primjenjiva u cijeloj Uniji 25. svibnja 2018., Uniji pruža alate potrebne za rješavanje slučajeva nezakonitog korištenja osobnih podataka u kontekstu izbora. No integritet demokratske politike očuvat će se samo čvrstom i dosljednom primjenom pravila. Budući da će se pravila prvi put primijeniti u kontekstu europskih izbora povodom skorašnjih izbora za Europski parlament, važno je osigurati jasnu sliku dionicima izbornog procesa –

¹ Izvješća tijela za zaštitu podataka u Ujedinjenoj Kraljevini (Ured povjerenika za informiranje – ICO) od 10. srpnja 2018.: „Investigation into the use of data analytics in political campaigns – Investigation update” i „Democracy Disrupted? Personal information and political influence”.

² https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

³ <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267> „Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall’informativa per fini di propaganda elettorale”, objavljeno u službenom glasilu talijanskog tijela za zaštitu podataka, br. 71, 26.3.2014. [doc. web n. 3013267]; <https://www.cnil.fr/fr/communication-politique-queles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux> „Communication politique: quelles sont les règles pour l’utilisation des données issues des réseaux sociaux?”, objavilo francusko nacionalno tijelo Commission Nationale de l’informatique et des libertés, 8.11.2016. ; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf, smjernice o političkim kampanjama Ureda povjerenika za informiranje [20170426].

⁴ Uredba (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 (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

nacionalnim izbornim tijelima, političkim strankama, posrednicima podataka i analitičarima, platformama društvenih mreža te internetskim oglašivačkim mrežama. Ovim smjernicama stoga se želi istaknuti obveze u kontekstu zaštite podataka koje su relevantne za izbore. Nacionalna tijela za zaštitu podataka koja provode Opću uredbu o zaštiti podataka moraju u potpunosti iskoristiti svoje ojačane ovlasti kako bi otklonila moguće povrede, posebno one povezane s mikrociljanjem.

1. Okvir Unije za zaštitu podataka

Zaštita osobnih podataka temeljno je pravo sadržano u Povelji Europske unije o temeljnim pravima (članak 8.) i u Ugovorima (članak 16. UFEU-a). Općom uredbom o zaštiti podataka jača se okvir za zaštitu podataka, Unija postaje bolje opremljena za rješavanje slučajeva zlouporabe osobnih podataka u budućnosti, a svi akteri odgovornije postupaju s osobnim podacima.

Građani u Uniji dobivaju dodatna i ojačana prava koja su posebno relevantna u kontekstu izbora. Na režim zaštite podataka koji je na snazi u Uniji posljednjih 20 godina posebno nepovoljno utječu fragmentirana primjena pravila u državama članicama, nedostatak formalnih mehanizama suradnje među nacionalnim tijelima za zaštitu podataka i ograničene izvršne ovlasti tih nadležnih tijela. Općom uredbom o zaštiti podataka otklanjaju se ti nedostaci: nadovezujući se na dokazana načela zaštite podataka usklađuju se ključna pitanja kao što je pristanak, jačaju se prava pojedinaca na primanje informacija o obradi njihovih podataka, razjašnjavaju se uvjeti pod kojima je moguće dodatno razmjenjivati osobne podatke, uvode se pravila o povredama osobnih podataka, uspostavlja se mehanizam suradnje između tijela za zaštitu podataka u prekograničnim slučajevima te se jačaju njihove izvršne ovlasti. U slučaju povrede pravila EU-a o zaštiti podataka tijela za zaštitu podataka imaju ovlasti istražiti slučaj (primjerice, mogu naložiti dostavu informacija, provoditi inspekcije u prostorijama voditelja i izvršitelja obrade) i ispraviti ponašanje (primjerice, izdavati upozorenja i opomene ili izreći privremenu ili konačnu obustavu obrade). Imaju i ovlast izricanja novčanih kazni u iznosu do 20 milijuna EUR ili, ako je riječ o poduzeću, do 4 % godišnjeg prometa na svjetskoj razini⁵. Pri odlučivanju o izricanju novčanih kazni i njihovoj razini, tijela za zaštitu podataka razmotrit će okolnosti pojedinačnog slučaja i čimbenike poput prirode, opsega ili svrhe obrade, broja pogođenih osoba i razine štete koju su pretrpjeli⁶. U kontekstu izbora vjerojatno će biti riječ o teškoj povredi kojom je pogođen veći broj osoba. To može voditi do izricanja visokih kazni, posebno uzimajući u obzir važnost pitanja povjerenja građana u demokratski proces.

Novoosnovani Europski odbor za zaštitu podataka, koji okuplja sva nacionalna tijela za zaštitu podataka te Europskog nadzornika za zaštitu podataka, ima ključnu ulogu u primjeni Opće uredbe o zaštiti podataka tako što izdaje smjernice, preporuke i primjere najbolje prakse⁷. Budući da su nacionalna tijela za zaštitu podataka zadužena za provođenje Opće

⁵ Smjernice Komisije o Općoj uredbi o zaštiti podataka na adresi: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_hr

⁶ Članak 83. Opće uredbe o zaštiti podataka.

⁷ Europski nadzornik za zaštitu podataka također izdaje mišljenja.

uredbe o zaštiti podataka i održavanje izravnih kontakata s dionicima, ta tijela mogu zajamčiti dodatnu pravnu sigurnost kad je riječ o tumačenju Uredbe. Komisija aktivno podupire to djelovanje.

Direktiva o privatnosti i elektroničkim komunikacijama ili „Direktiva o e-privatnosti” (Direktiva 2002/58/EZ Europskog parlamenta i Vijeća⁸) dopunjuje okvir Unije za zaštitu podataka te je relevantna u kontekstu izbora jer njezino područje primjene obuhvaća pravila o elektroničkom slanju nezatraženih komunikacija, uključujući u svrhu izravnog marketinga. Direktivom o e-privatnosti utvrđuju se i pravila o pohrani informacija i pristupu informacijama koje su već pohranjene (u terminalnoj opremi kao što su pametni telefon ili računalo), kao što su kolačići s pomoću kojih je moguće pratiti ponašanje korisnika na internetu. Komisijin Prijedlog uredbe o privatnosti i elektroničkim komunikacijama (Uredba o e-privatnosti)⁹, o kojem se trenutačno pregovara, temelji se na istim načelima kao i Direktiva o e-privatnosti. Novom uredbom područje njezine primjene proširit će se tako da osim tradicionalnih telekomunikacijskih operatera obuhvati i usluge elektroničke komunikacije na internetu.

2. Ključne obveze raznih aktera

Opća uredba o zaštiti podataka primjenjuje se na sve aktere koji aktivno djeluju u kontekstu izbora, kao što su europske i nacionalne političke stranke (dalje u tekstu „političke stranke”), europske i nacionalne političke zaklade (dalje u tekstu „zaklade”), platforme, poduzeća za podatkovnu analitiku i javna tijela odgovorna za izborni proces. Oni moraju obrađivati osobne podatke (primjerice imena i adrese) zakonito, pravedno i transparentno i samo u navedene svrhe. Ne mogu ih dalje upotrebljavati na način koji nije sukladan namjenama za koje su podaci prvotno prikupljeni. I obrada u novinarske svrhe obuhvaćena je područjem primjene Opće uredbe o zaštiti podataka, no na nju mogu povoljno utjecati iznimke i odstupanja predviđeni nacionalnim pravom, s obzirom na važnost prava na slobodu izražavanja i informiranja u demokratskom društvu¹⁰.

Osobni podaci sveobuhvatan su pojam. Osobni podaci su svi podaci o identificiranoj fizičkoj osobi ili fizičkoj osobi koju je moguće identificirati. Podaci koji se obrađuju u kontekstu izbora često će uključivati posebne kategorije osobnih podataka („osjetljivi podaci”) kao što su podaci o političkim uvjerenjima, članstvu u sindikatu, etničkom podrijetlu, seksualnom životu itd., a takve je podatke potrebno bolje zaštititi¹¹. Štoviše, s pomoću podatkovne analitike moguće je iz skupova podataka koji nisu osjetljive prirode izvesti „osjetljive podatke” (primjerice podatke o političkim, ali i vjerskim uvjerenjima ili spolnoj orijentaciji). I

⁸ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

⁹ Prijedlog uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama) (COM(2017) 10 final).

¹⁰ Članak 85. stavak 2. Opće uredbe o zaštiti podataka.

¹¹ Članak 9. stavak 1. Opće uredbe o zaštiti podataka.

obrada tih izvedenih podataka obuhvaćena je područjem primjene Opće uredbe o zaštiti podataka i stoga bi trebala biti usklađena sa svim pravilima o zaštiti podataka.

Dakle, gotovo svi postupci obrade podataka u kontekstu izbora podliježu Općoj uredbi o zaštiti podataka.

Uzimajući u obzir da akteri u izbornom procesu moraju imati jasnu sliku te uzimajući u obzir prve nalaze u slučaju poduzeća Cambridge Analytica, u sljedećim su odjeljcima istaknute obveze u vezi sa zaštitom podataka koje se čine posebno važnima u kontekstu izbora. One su sažete u prilogu.

2.1 Voditelji i izvršitelji obrade

Središnji element Opće uredbe o zaštiti podataka jest koncept odgovornosti voditelja i zajedničkih voditelja obrade. Voditelj obrade podataka organizacija je koja odlučuje, sama ili u suradnji s drugima, zašto se i kako osobni podaci obrađuju; izvršitelj obrade podataka obrađuje osobne podatke samo u ime i po nalogu voditelja obrade (njihov odnos utvrđen je ugovorom ili drugim pravno obvezujućim aktom). Voditelji obrade podataka moraju uvesti mjere razmjerne rizicima i od samog početka u proces obrade integrirati zaštitu podataka; moraju moći dokazati usklađenost s Općom uredbom o zaštiti podataka (načelo odgovornosti).

Ulogu voditelja ili izvršitelja obrade podataka treba ocijeniti u svakom pojedinom slučaju. U kontekstu izbora razni akteri mogu biti voditelji obrade podataka: političke stranke, pojedinačni kandidati i zaklade najčešće su voditelji obrade podataka; platforme i poduzeća za podatkovnu analitiku mogu biti (zajednički) voditelji ili izvršitelji obrade za određenu obradu ovisno o stupnju kontrole nad predmetnom obradom¹²; nacionalna izborna tijela vode obradu za izborne registre.

Ako se aktivnosti obrade odnose na ponudu roba i usluga pojedincima u Uniji ili praćenje njihova ponašanja u Uniji, i poduzeća sa sjedištem izvan Unije moraju se uskladiti s Općom uredbom o zaštiti podataka. To vrijedi za niz platformi i poduzeća za podatkovnu analitiku.

2.2 Načela, zakonitost obrade i posebni uvjeti za „osjetljive podatke”

Subjekti koji sudjeluju u izborima mogu obrađivati osobne podatke, uključujući podatke dobivene iz javnih izvora, samo u skladu s načelima povezanima s obradom osobnih podataka i na temelju ograničenog broja razloga koji su jasno utvrđeni u Općoj uredbi o zaštiti podataka¹³. Najvažniji razlozi za zakonitu obradu u kontekstu izbora obuhvaćaju pristanak pojedinca, usklađenost s pravnim obvezama prema zakonodavstvu Unije ili nacionalnom zakonodavstvu, izvršavanje zadaće u javnom interesu i legitimni interes jednog od subjekata.

¹² Najnovijom sudskom praksom Suda Europske unije (Jehovini svjedoci, predmet C-25/17, presuda od 10. srpnja 2018.) pojašnjeno je da se organizacija koja utječe na aktivnosti prikupljanja i obrade osobnih podataka može, u određenim okolnostima, smatrati voditeljem obrade.

¹³ Članci 5. i 6. Opće uredbe o zaštiti podataka.

No subjekti u kontekstu izbora mogu se pozvati na legitimni interes samo ako njihove interese ne nadjačavaju interesi predmetnih pojedinaca ili njihova temeljna prava i slobode.

K tomu, pohrana informacija u terminalnoj opremi (računalo, pametni telefon itd.), ili stjecanje pristupa informacijama koje su već pohranjene, mora biti u skladu sa zahtjevima Direktive o e-privatnosti za zaštitu terminalne opreme, što znači da bi predmetni pojedinac morao dati svoj pristanak.

Ako je pravna osnova obrade pristanak, Općom uredbom o zaštiti podataka propisan je jasan i nedvosmislen pristanak koji mora biti slobodan i informiran¹⁴.

Javna tijela uključena u kontekst izbora obrađuju osobne podatke kako bi poštovala pravnu obvezu ili kako bi izvršavala javnu zadaću. Drugi subjekti u kontekstu izbora mogu obrađivati podatke na temelju pristanka ili legitimnog interesa¹⁵. Političke stranke i zaklade također mogu obrađivati podatke na temelju javnog interesa ako je tako predviđeno nacionalnim pravom¹⁶.

Javna tijela mogu otkriti političkim strankama određene podatke o pojedincima uvrštenima na izborne liste ili u registre rezidenata samo ako im je to izričito dopušteno pravom države članice i samo u svrhu oglašavanja u kontekstu izbora i u mjeri u kojoj je to nužno za tu svrhu; primjerice mogu otkriti ime i adresu.

Obrada u kontekstu izbora često će uključivati „osjetljive podatke”. Obrada takvih podataka, uključujući izvedene „osjetljive podatke”, općenito je zabranjena osim ako se primjenjuje neko od posebnih obrazloženja predviđenih Općom uredbom o zaštiti podataka¹⁷. Obrada „osjetljivih” podataka zahtijeva ispunjenje specifičnih, strožih uvjeta: osoba mora dati izričitu suglasnost¹⁸ ili mora dotične podatke učiniti javnima¹⁹. Političke stranke i zaklade također mogu obrađivati „osjetljive podatke” ako postoji znatan javni interes na temelju prava Unije ili države članice te ako su na snazi odgovarajuće zaštitne mjere²⁰. Općom uredbom o zaštiti podataka predviđeno je da i one mogu obrađivati „osjetljive podatke” u mjeri u kojoj je to isključivo povezano s njihovim članovima ili bivšim članovima ili osobama koje su s njima u redovitom kontaktu – no podaci se mogu otkriti samo u okviru njihove političke stranke ili zaklade²¹. No politička stranka ne može primijeniti tu specifičnu odredbu za obradu podataka o budućim članovima ili glasačima.

¹⁴ Članak 7. i članak 4. stavak 11. Opće uredbe o zaštiti podataka.

¹⁵ Pod uvjetom da prava i slobode dotičnih pojedinaca nisu ozbiljno narušeni.

¹⁶ Vidjeti uvodnu izjavu 56. Opće uredbe o zaštiti podataka: „Ako tijekom izbornih aktivnosti djelovanje demokratskog sustava u državi članici zahtijeva da političke stranke prikupljaju osobne podatke o političkim mišljenjima ljudi, obrada takvih podataka može se dopustiti iz razloga javnog interesa, pod uvjetom da se uspostave odgovarajuće zaštitne mjere.”

¹⁷ Članak 9. Opće uredbe o zaštiti podataka.

¹⁸ Članak 9. stavak 2. točka (a) Opće uredbe o zaštiti podataka.

¹⁹ Članak 9. stavak 2. točka (e) Opće uredbe o zaštiti podataka.

²⁰ Članak 9. stavak 2. točka (g) Opće uredbe o zaštiti podataka.

²¹ Članak 9. stavak 2. točka (d) Opće uredbe o zaštiti podataka. Politička stranka ili zaklada ne može dijeliti s trećom stranom podatke koji se odnose na njihove članove ili bivše članove ili osobe koje imaju redovit kontakt s njima, ako predmetni pojedinac na to ne pristane.

Svrha obrade podataka trebala bi biti utvrđena u vrijeme prikupljanja (načelo „ograničavanja svrhe”)²². Podaci prikupljeni u jednu svrhu mogu se dalje obrađivati samo u kompatibilnu svrhu; u suprotnom je za obradu u novu svrhu potrebno navesti novu pravnu osnovu predviđenu Općom uredbom o zaštiti podataka. Posebno, kada posrednici podataka o stilu života ili platforme prikupljaju podatke u komercijalne svrhe, te podatke nije moguće dalje obrađivati u kontekstu izbora.

Osim ako političke stranke i zaklade s dužnom pažnjom provjere jesu li podaci zakonito pribavljeni, ne mogu se koristiti takvim podacima dobivenima od treće strane.

2.3 Zahtjevi za transparentnost

Slučaj poduzeća Cambridge Analytica pokazao je važnost borbe protiv netransparentnosti i pravilnog informiranja pojedinaca kojih se to tiče. Pojedinci često ne znaju tko obrađuje njihove osobne podatke i u koje svrhe. Prema načelima poštene i transparentne obrade ispitanik treba biti informiran o postupku obrade i njegovim svrhama²³. Općom uredbom o zaštiti podataka objašnjavaju se obveze voditelja obrade u tom smislu. Oni moraju obavijestiti pojedince o ključnim aspektima koji se odnose na obradu njihovih osobnih podataka kao što su:

- identitet voditelja obrade;
- svrhe obrade;
- primatelji osobnih podataka;
- izvor podataka ako se oni ne prikupljaju izravno od osobe;
- postojanje automatiziranog donošenja odluka i
- eventualne daljnje informacije potrebne kako bi se osigurala poštena i transparentna obrada²⁴.

Štoviše, Općom uredbom o zaštiti podataka propisano je da se te informacije daju u sažetom, transparentnom, razumljivom i lako dostupnom obliku te da se rabi jasan i jednostavan jezik²⁵. Primjerice, kratka i nejasna obavijest o zaštiti podataka otisnuta sitnim slovima na izbornim materijalima ne bi bila u skladu sa zahtjevima u pogledu transparentnosti.

Prema prvim nalazima, ključni nedostatak u slučaju poduzeća Cambridge Analytica odnosio se na nepotpune informacije o svrsi u koju su podaci prikupljeni, a to je dovelo u pitanje i valjanost suglasnosti osoba čiji su se podaci prikupljali. Sve organizacije koje obrađuju osobne podatke u kontekstu izbora moraju se pobrinuti da pojedinci u potpunosti shvaćaju kako će se njihovi osobni podaci upotrebljavati i u koju svrhu, prije no što daju pristanak ili prije početka obrade voditelja obrade na temelju bilo kojeg drugog razloga.

Pojedincima je potrebno pružiti informacije u svakoj fazi obrade, a ne samo kada se podaci prikupe.

²² Članak 5. stavak 1. točka (b) Opće uredbe o zaštiti podataka.

²³ Članak 5. stavak 1. točka (a) Opće uredbe o zaštiti podataka.

²⁴ Članci 13. i 14. Opće uredbe o zaštiti podataka.

²⁵ Smjernice o transparentnosti Europskog odbora za zaštitu podataka.

Posebno, kada političke stranke obrađuju podatke dobivene od trećih strana (primjerice iz izbornih registara, od posrednika podataka, analitičara podataka i drugih izvora) obično moraju obavijestiti pojedince na koje se podaci odnose i objasniti im kako ih kombiniraju i upotrebljavaju da bi se osigurala pravedna obrada²⁶.

2.4 Profiliranje, automatizirano donošenje odluka i mikrociljanje

Profiliranje je oblik automatizirane obrade podataka koji se koristi za analizu ili predviđanje aspekata koji se odnose na osobne preference, interese, gospodarsku situaciju itd.²⁷ Profiliranje se može upotrebljavati za mikrociljanje, konkretno za analizu osobnih podataka (kao što je povijest pretraživanja na internetu) radi utvrđivanja konkretnih interesa određene publike ili pojedinca u cilju utjecanja na njihove postupke. Mikrociljanje se može upotrebljavati za pružanje personalizirane poruke pojedincu ili publici s pomoću internetskih usluga, npr. društvenih mreža.

Slučaj poduzeća Cambridge Analytica pokazao je posebna pitanja koja se nameću zbog metoda mikrociljanja na društvenim mrežama. Organizacije mogu rudariti podatke prikupljene od korisnika društvenih mreža kako bi izradile profile glasača. To bi im moglo omogućiti da identificiraju glasače na koje se može lakše utjecati te da tako utječu na ishod izbora.

Na takvu obradu podataka primjenjuju se sva opća načela i pravila Opće uredbe o zaštiti podataka, primjerice načela zakonitosti, pravednosti i transparentnosti te ograničavanja svrhe. Pojedinci često nisu svjesni toga da se izrađuju njihovi profili: ne razumiju zašto primaju neke oglase koji su tako jasno povezani s njihovim posljednjim pretragama ili zašto primaju personalizirane poruke od različitih organizacija. Opća uredba o zaštiti podataka obvezuje sve voditelje obrade, primjerice političke stranke ili analitičare podataka, da obavijeste pojedince kada rabe takve tehnike i o njihovim posljedicama²⁸.

U Općoj uredbi o zaštiti podataka prepoznato je da automatizirano donošenje odluka, što obuhvaća profiliranje, može imati ozbiljne posljedice. Općom uredbom o zaštiti podataka predviđeno je da pojedinac ima pravo da ne bude podvrgnut odluci temeljenoj isključivo na automatiziranoj obradi kojom nastaju pravni učinci koji se odnose na njega ili slični znatni učinci, osim ako se takva obrada provodi u strogim uvjetima, točnije kada pojedinci daju izričit pristanak ili ako je to omogućeno pravom Unije ili države članice u kojem su utvrđene odgovarajuće zaštitne mjere²⁹.

Praksa mikrociljanja u kontekstu izbora ubraja se u ovu kategoriju ako njome nastaje dovoljno izražen učinak na pojedince. Europski odbor za zaštitu podataka utvrdio je da je to slučaj ako odluka ima potencijal da znatno utječe na okolnosti, ponašanje ili izbore pojedinaca ili ima

²⁶ Članak 14. Opće uredbe o zaštiti podataka.

²⁷ Kao što je definirano u članku 4. stavku 4. Opće uredbe o zaštiti podataka.

²⁸ Članak 13. stavak 2. Opće uredbe o zaštiti podataka.

²⁹ Članak 22. Opće uredbe o zaštiti podataka.

produljen ili trajan utjecaj na pojedinca³⁰. Odbor je smatrao da bi ciljano internetsko oglašavanje u nekim okolnostima moglo u dovoljnoj mjeri utjecati na pojedince ako je, primjerice, nametljivo ili se njime iskorištavaju znanje ili ranjivosti pojedinca. S obzirom na važnost ostvarivanja demokratskog prava na glasovanje, personalizirane poruke kojima bi se, primjerice, pojedince moglo spriječiti da glasaju ili ih navesti da glasaju na određeni način, mogle bi ispunjavati kriterij izraženog učinka.

U kontekstu izbora voditelji obrade moraju osigurati zakonitost svake obrade u kojoj se primjenjuju takve tehnike u skladu s gore navedenim načelima i strogim uvjetima Opće uredbe o zaštiti podataka.

2.5 Sigurnost i točnost osobnih podataka

Sigurnost je posebno važna u kontekstu izbora s obzirom na veličinu obuhvaćenih skupova podataka i činjenicu da oni često sadržavaju „osjetljive podatke”. Općom uredbom o zaštiti podataka od operatera koji obrađuju osobne podatke (i od voditelja i od izvršitelja obrade) zahtijeva se uvođenje odgovarajućih tehničkih i organizacijskih mjera kako bi se osigurala razina sigurnosti primjerena rizicima za prava i slobode pojedinaca koji nastaju obradom³¹.

Općom uredbom o zaštiti podataka od voditelja obrade zahtijeva se da obavijeste nadležno nadzorno tijelo o povredama osobnih podataka bez nepotrebne odgode, a najkasnije u roku od 72 sata. Ako će povreda osobnih podataka vjerojatno uzrokovati velik rizik za prava i slobode pojedinaca, voditelj mora obavijestiti i pojedince na koje ta povreda utječe, bez nepotrebne odgode³².

Političke stranke i drugi dionici uključeni u izborni proces moraju posebno paziti na točnost osobnih podataka pri obradi velikih skupova podataka i kada se podaci prikupljaju iz različitih, heterogenih izvora. Netočne podatke potrebno je odmah izbrisati ili ispraviti, a po potrebi i ažurirati.

2.6 Procjena učinka na zaštitu podataka

Općom uredbom o zaštiti podataka uvodi se novi alat za procjenu rizika prije početka obrade, a to je procjena učinka na zaštitu podataka. Ta je procjena učinka nužna svaki put kad bi obrada vjerojatno mogla prouzročiti visok rizik za prava i slobode pojedinaca³³. To se događa, primjerice, u kontekstu izbora kada voditelj obrade podataka sustavno i opsežno ocjenjuje osobne aspekte pojedinca (uključujući profiliranje), što na njega znatno utječe, te kada voditelj obrade obrađuje veliku količinu „osobnih podataka”. Nacionalna izborna tijela koja izvršavaju svoje javne zadaće možda neće morati provoditi procjenu učinka na zaštitu podataka ako je ona već provedena u kontekstu donošenja zakonodavstva.

³⁰ Smjernice Europskog odbora za zaštitu podataka o automatiziranom donošenju odluka, WP251rev.01, kako su zadnje izmijenjene i donesene 6.2.2018.

³¹ Članak 32. Opće uredbe o zaštiti podataka.

³² Članci 33. i 34. Opće uredbe o zaštiti podataka; i Smjernice Europskog odbora za zaštitu podataka o obavješćivanju o povredi osobnih podataka.

³³ Članci 35. i 36. Opće uredbe o zaštiti podataka; i Smjernice Europskog odbora za zaštitu podataka o procjeni učinka na zaštitu podataka.

Procjene učinka koje različiti dionici moraju provesti u kontekstu izbora trebale bi obuhvaćati elemente nužne za otklanjanje rizika obuhvaćenih takvom obradom, posebno zakonitost obrade i za skupove podataka dobivene od trećih strana te zahtjeve transparentnosti.

3. Prava pojedinaca

Općom uredbom o zaštiti podataka pojedincima se daju dodatna i veća prava koja su posebno relevantna u kontekstu izbora:

- pravo na pristup vlastitim osobnim podacima;
- pravo da zatraže brisanje osobnih podataka ako se obrada temelji na pristanku i taj se pristanak povuče, ako podaci više nisu potrebni ili ako je njihova obrada nezakonita; i
- pravo na ispravak netočnih ili nepotpunih osobnih podataka.

Pojedinci imaju pravo uložiti prigovor na obradu (primjerice, obradu podataka uvrštenih u izborne popise koji se prenose političkim strankama) ako se obrada njihovih podataka temelji na „legitimnom interesu” ili „javnom interesu”.

Pojedinci imaju pravo da ne podliježu odlukama koje se temelje isključivo na automatiziranoj obradi njihovih osobnih podataka. U takvim slučajevima pojedinac može zatražiti intervenciju fizičke osobe i ima pravo izraziti svoje stajalište i osporiti odluku.

Kako bi pojedinci mogli ostvariti ta prava, svi uključeni dionici moraju osigurati potrebne alate i postavke. Općom uredbom o zaštiti podataka predviđa se mogućnost izrade kodeksa ponašanja koji odobrava tijelo za zaštitu podataka, a u njemu se određuje primjena Uredbe u posebnim područjima, uključujući u kontekstu izbora.

Općom uredbom o zaštiti podataka pojedincima se daje pravo na podnošenje pritužbe nadzornom tijelu i pravo na pravni lijek. Pojedincima se ujedno daje pravo da ovlaste nevladinu organizaciju da u njihovo ime podnese pritužbu³⁴. U nekim državama članicama nacionalnim zakonodavstvom omogućuje se nevladinoj organizaciji da podnese pritužbu i ako je pojedinac nije za to ovlastio. To je posebno važno u kontekstu izbora s obzirom na to da bi to moglo utjecati na velik broj osoba.

³⁴ Članak 80. stavak 1. Opće uredbe o zaštiti podataka.

Ključna pitanja o zaštiti podataka koja su relevantna u izbornom procesu³⁵

Političke stranke i zaklade	Političke stranke i zaklade su voditelji obrade podataka.	
	• U svom djelovanju poštuju načelo ograničavanja svrhe, a daljnja obrada provodi se samo u kompatibilne svrhe (primjerice, pri razmjeni podataka s platformama). • Odabiru odgovarajuću pravnu osnovu za obradu podataka (i za izvedene podatke): pristanak, legitimni interes, zadaća u javnom interesu (ako je propisano zakonom), posebni uvjeti za „osjetljive podatke” (primjerice: politički stav). • Procjenjuju učinak na zaštitu podataka. • Obavješćuju pojedince o svrsi svake obrade (zahtjevi za transparentnost), bilo da se podaci prikupljaju izravno ili se dobivaju od trećih strana. • Osiguravaju točnost podataka, posebno ako je riječ o podacima iz različitih izvora i izvedenim podacima. • Provjeravaju jesu li podaci od trećih strana dobiveni zakonito i u koju svrhu (primjerice: jesu li dotični pojedinci dali svoj informirani pristanak za određenu svrhu). • Uzimaju u obzir posebne rizike koji proizlaze iz profiliranja i donose odgovarajuće zaštitne mjere. • Usklađuju se s posebnim uvjetima pri uporabi automatiziranog donošenja odluka (primjerice, dobivanje izričitog pristanka i uvođenje prikladnih zaštitnih mjera). • Jasno utvrđuju tko ima pristup podacima. • Jamče sigurnost obrade s pomoću tehničkih i organizacijskih mjera; prijavljuju povrede podataka. • Razjašnjavaju obveze u ugovorima ili drugim pravno obvezujućim aktima s izvršiteljima obrade podataka, kao što su poduzeća za podatkovnu analitiku. • Brišu podatke kada više nisu potrebni u prvobitne svrhe u koje su prikupljeni.	
	Posrednici podataka i poduzeća za podatkovnu analitiku su (zajednički) voditelji ili izvršitelji obrade podataka ovisno o stupnju kontrole koju imaju nad postupkom obrade.	
	Voditelj obrade	Izvršitelj obrade
	• Poštuje ograničavanje svrhe; daljnja obrada samo u sukladne svrhe (osobito ako se podaci dijele s	• Poštuje obveze iz ugovora ili drugog pravnog akta s voditeljem.

³⁵ Gore navedene informacije nisu iscrpne. Navode se kako bi se naglasio niz ključnih obveza povezanih s podacima u skladu s Općom uredbom o zaštiti podataka, koje su relevantne u izbornom procesu. U skladu su sa scenarijem u kojem političke stranke same prikupljaju podatke (iz javnih izvora, s društvenih mreža, izravno od birača itd.) i upotrebljavaju usluge posrednika podataka ili poduzeća za podatkovnu analitiku kako bi dosegle glasače putem društvenih mreža. Društvene mreže mogu biti izvor podataka za navedene subjekte. I drugo zakonodavstvo moglo bi biti relevantno, primjerice pravila o slanju nezatraženih komunikacija i pitanje zaštite terminalne opreme u Direktivi o e-privatnosti.

	trećim stranama). • Odabire odgovarajuću pravnu osnovu za obradu: pristanak, legitimni interes. Ako je riječ o osjetljivim podacima, obrada je moguća samo ako postoji izričit pristanak ili se podaci očigledno objavljuju. • Procjenjuje učinak na zaštitu podataka. • Obavještava pojedince o svakoj svrsi obrade (zahtjevi za transparentnost) – posebno ako se traži pristanak jer će se podaci obično prodati trećoj strani. • Pridržava se posebnih uvjeta pri uporabi automatiziranog donošenja odluka (npr. pribavljanje izričitog pristanka i uvođenje prikladnih zaštitnih mjera). • Posebno pazi na zakonitost obrade i točnost, ako se kombiniraju različiti skupovi podataka. • Osigurava sigurnost obrade s pomoću tehničkih i organizacijskih mjera; prijavljuje povrede podataka.	• Jamči sigurnost obrade s pomoću tehničkih i organizacijskih mjera. • Daje podršku voditelju obrade u procjeni učinka na zaštitu podataka ili ostvarivanju prava ispitanika ili tako što voditelja obrade odmah obavještuje o povredi podataka ako postane svjestan te povrede.
	Platforme su obično voditelji obrade podataka ako se na njima odvija obrada, a obradu mogu voditi zajednički s drugim organizacijama.	
Platforme društvenih mreža / internetske oglašivačke mreže	• Odabiru odgovarajuću pravnu osnovu za obradu: ugovor s pojedincima, pristanak, legitimni interes. Ako je riječ o osjetljivim podacima, obrada je moguća samo ako postoji izričit pristanak ili se podaci očigledno objavljuju. • Upotrebljavaju samo podatke potrebne za utvrđenu svrhu. • Procjenjuju učinak na zaštitu podataka. • Osiguravaju zakonitost ako se podaci o članovima dijele s trećim stranama. • Pridržavaju se zahtjeva transparentnosti, posebno s obzirom na Uvjete i odredbe, ako se podaci naknadno dijele s trećim stranama itd. • Pridržava se posebnih uvjeta pri uporabi automatiziranog donošenja odluka (npr. pribavljanje izričitog pristanka i uvođenje prikladnih zaštitnih mjera). • Jamče sigurnost obrade s pomoću tehničkih i organizacijskih mjera; prijavljuju povrede podataka. • Pojedincima daju kontrole i postavke za djelotvorno ostvarivanje njihovih prava, uključujući pravo da ne budu predmetom odluke koja se isključivo temelji na automatiziranoj obradi kao što je	

	profiliranje.
	Nacionalna izborna tijela su voditelji obrade podataka.
Nacionalna izborna tijela	• Pravna osnova za obradu: pravna obveza ili zadaća od javnog interesa na temelju zakona. • Provode procjenu učinka na zaštitu podataka ako učinak već nije procijenjen zakonom.