KOMISJA
EUROPEJSKA

Bruksela, dnia 12.9.2018 r.
COM(2018) 638 final

Wolne i uczciwe wybory

WYTYCZNE

Wytyczne Komisji dotyczące stosowania unijnych przepisów o ochronie danych osobowych w kontekście wyborczym

Wkład Komisji Europejskiej na spotkanie przywódców w Salzburgu w dniach 19-20 września 2018 r.

WYTYCZNE KOMISJI DOTYCZĄCE STOSOWANIA UNIJNYCH PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH W KONTEKŚCIE WYBORCZYM

Proces demokratyczny nie może funkcjonować bez udziału obywateli. Partie polityczne nieustannie komunikują się z elektoratem, dostosowując do niego swój przekaz oraz uwzględniając wyrażane przez wyborców interesy. Dlatego też jest czymś oczywistym, że podmioty biorące udział w procesie wyborczym interesują się takim wykorzystaniem danych, które może przynieść sukces wyborczy. Rozwój narzędzi cyfrowych i platform internetowych otworzył wiele nowych możliwości angażowania społeczeństwa w debatę polityczną.

Jednakże zastosowanie techniki tzw. mikrotargetowania wyborców, która wiąże się z niezgodnym prawem przetwarzaniem danych osobowych (co można było zaobserwować w ujawnionej aferze Cambridge Analytica), to już zupełnie inny co do istoty problem. Pokazuje on, z jakimi wyzwaniami wiąże się stosowanie nowoczesnych technologii, ale jednocześnie podkreśla szczególne znaczenie ochrony danych w kontekście wyborczym. Problem ten stał się kluczową kwestią nie tylko dla każdego z nas, ale również dla funkcjonowania naszych demokracji, ponieważ stanowi on poważne zagrożenie dla sprawiedliwego i demokratycznego procesu wyborczego oraz może przyczyniać się do podważania takich zasad jak otwartość w debacie, uczciwość i przejrzystość, niezbędnych dla ustroju demokratycznego. Zdaniem Komisji niezwykle istotne jest, aby zająć się tą kwestią w celu przywrócenia zaufania publicznego do uczciwego procesu wyborczego.

Pierwsze sprawozdania brytyjskiego urzędu ochrony danych (Biuro Komisarza ds. informacji – ICO) na temat wykorzystywania danych do analiz na potrzeby kampanii politycznych[1] oraz opinia Europejskiego Inspektora Ochrony Danych w sprawie manipulacji online i danych osobowych[2] potwierdziły rosnący wpływ mikrotargetowania, które opracowano do celów handlowych, w kontekście wyborczym.

W ogólniejszym ujęciu kwestią ochrony danych w kontekście wyborczym zajmowało się szereg organów ochrony danych[3].

Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady (ogólne rozporządzenie o ochronie danych)[4], które ma bezpośrednie zastosowanie w całej Unii od dnia 25 maja

[1] Sprawozdania brytyjskich organów ochrony danych (Biuro Komisarza ds. Ochrony Danych – ICO) z dnia 10 lipca 2018 r.: „Badanie dotyczące stosowania analizy danych w kampaniach politycznych – badanie zaktualizowane" oraz „Czy demokracja została zakłócona"? Dane osobowe a wywieranie wpływu politycznego".

[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" opublikowane w Dzienniku Urzędowym włoskiego Urzędu Ochrony Danych numer 71 w dniu 26.03.2014 r. [doc. web n. 3013267]; https://www.cnil.fr/fr/communication-politique-quelles-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?" opublikowane przez francuską Krajową Komisję ds. Technologii Informatycznych i Swobód (Commission Nationale de l'informatique et des libertés) 08.11.2016; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office 'Guidance on political campaigning' [20170426].

2018 r., zapewnia Unii narzędzia niezbędne do przeciwdziałania przypadkom niezgodnego z prawem wykorzystywania danych osobowych w kontekście wyborczym. Tylko jednak zdecydowane i spójne stosowanie tych przepisów przyczyni się do ochrony integralności polityki demokratycznej. Ponieważ przepisy te po raz pierwszy znajdą zastosowanie w kontekście wyborów europejskich, przy okazji zbliżających się wyborów do Parlamentu Europejskiego, istotne jest stworzenie podmiotom zaangażowanym w proces wyborczy – takim jak krajowe organy wyborcze, partie polityczne, brokerzy baz danych, analitycy danych, czy internetowe sieci reklamy online – klarownych zasad działania. Celem niniejszych wytycznych jest podkreślenie obowiązków w zakresie ochrony danych mających znaczenie dla wyborów. Krajowe organy ochrony danych, których zadaniem jest egzekwowanie ogólnego rozporządzenia o ochronie danych, powinny w pełni wykorzystywać przysługujące im wzmocnione uprawnienia władcze, aby zwalczać ewentualne naruszenia w tym zakresie, w szczególności te odnoszące się do mikrotargetowania wyborców.

1. Unijne ramy ochrony danych

Ochrona danych osobowych jest prawem podstawowym zagwarantowanym w Karcie praw podstawowych Unii Europejskiej (art. 8) oraz w traktatach (art. 16 TFUE). Ogólne rozporządzenie o ochronie danych wzmacnia ramy ochrony danych, wyposażając Unię w lepsze narzędzia służące zwalczaniu przypadków nadużyć w zakresie danych osobowych w przyszłości oraz wprowadzając większą odpowiedzialność oraz rozliczalność wszystkich podmiotów za to, jak przetwarzają one dane osobowe.

Rozporządzenie to przyznaje osobom fizycznym w Unii dodatkowe i większe prawa, które nabierają szczególnego znaczenia w kontekście wyborów. Reżim prawny ochrony danych, który w ostatnich 20 latach obowiązywał w Unii, dotknięty był niedostatkami, w szczególności z uwagi na stosowanie w sposób fragmentaryczny przepisów pomiędzy państwami członkowskimi, brak sformalizowanych mechanizmów współpracy krajowych organów ochrony danych oraz ze względu na ograniczone uprawnienia w zakresie egzekwowania prawa, jakimi dysponowały te organy. Ogólne rozporządzenie o ochronie danych odnosi się do tych niedociągnięć: opierając się na sprawdzonych zasadach ochrony danych, harmonizuje ono kluczowe pojęcia, takie jak zgoda, zwiększa prawa osób fizycznych do otrzymywania informacji na temat przetwarzania ich danych, precyzuje warunki, na jakich dane osobowe można dalej udostępniać, wprowadza przepisy dotyczące naruszeń danych, ustanawia mechanizm współpracy między organami ochrony danych w sprawach transgranicznych oraz wzmacnia ich uprawnienia w zakresie egzekwowania prawa. W przypadku naruszenia unijnych przepisów o ochronie danych organy ochrony danych mają uprawnienia do prowadzenia dochodzeń (np. poprzez zobowiązanie do udzielania informacji, przeprowadzanie kontroli w pomieszczeniach administratorów i podmiotów przetwarzających) oraz do korygowania zachowań (np. poprzez wydawanie ostrzeżeń i nagan, bądź też nakładanie zawieszeń przetwarzania o charakterze tymczasowym lub ostatecznym).

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

Mają one również uprawnienia do nakładania kar pieniężnych w wysokości do 20 mln EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu[5]. Podejmując decyzję o nałożeniu kary pieniężnej oraz jej wysokości, organy ochrony danych uwzględnią okoliczności danej sprawy oraz takie elementy, jak charakter, zakres lub cel przetwarzania, liczba osób, których to dotyczy, a także rozmiar poniesionych przez nie szkód[6]. Jeżeli chodzi o wybory, prawdopodobne jest, że waga naruszenia oraz liczba osób, których ono dotyczy, będą znaczne. Może to doprowadzić do nałożenia wysokich kar, w szczególności biorąc pod uwagę znaczenie kwestii zaufania obywateli do procesu demokratycznego.

Niedawno utworzona Europejska Rada Ochrony Danych, w której skład wchodzą wszystkie krajowe organy ochrony danych oraz Europejski Inspektor Ochrony Danych, odgrywa kluczową rolę w stosowaniu ogólnego rozporządzenia o ochronie danych poprzez wydawanie wytycznych, zaleceń i najlepszych praktyk[7]. Krajowe organy ochrony danych egzekwują stosowanie rozporządzenia oraz są bezpośrednimi punktami kontaktowymi dla zainteresowanych podmiotów. Dlatego to one właśnie są w stanie w najlepszy sposób zapewnić większą pewność prawa, jeżeli chodzi o interpretowanie rozporządzenia. Komisja aktywnie wspiera organy krajowe w tym zakresie.

Dyrektywa o prywatności i łączności elektronicznej (dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady [8]) uzupełnia unijne ramy ochrony danych i ma duże znaczenie w kontekście wyborczym, ponieważ jej zakres przedmiotowy obejmuje zasady dotyczące elektronicznego przesyłania niezamówionych komunikatów, w tym komunikatów do celów marketingu bezpośredniego. Dyrektywa o prywatności i łączności elektronicznej określa również zasady przechowywania informacji i uzyskiwania dostępu do już przechowywanych informacji, takich jak pliki cookie, które mogą być wykorzystywane do śledzenia zachowań użytkowników w sieci, w urządzeniach końcowych, takich jak smartfon lub komputer. Wniosek Komisji dotyczący rozporządzenia o prywatności i łączności elektronicznej[9], który obecnie jest przedmiotem negocjacji, opiera się na tych samych zasadach, co dyrektywa o prywatności i łączności elektronicznej. Nowe rozporządzenie rozszerzy swój zakres podmiotowy poza tradycyjnych operatorów telekomunikacyjnych, aby objąć podmioty świadczące internetowe usługi łączności elektronicznej.

[5] Wytyczne Komisji dotyczące stosowania ogólnego rozporządzenia o ochronie danych dostępne tutaj: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pl

[6] Art. 83 ogólnego rozporządzenia o ochronie danych.

[7] Europejski Inspektor Ochrony Danych wydaje również opinie.

[8] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

[9] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final.

2. Kluczowe obowiązki różnych podmiotów

Ogólne rozporządzenie o ochronie danych stosuje się do wszystkich podmiotów działających w kontekście wyborczym, takich jak europejskie i krajowe partie polityczne (zwane dalej: „partiami politycznymi"), europejskie i krajowe fundacje polityczne (zwane dalej: „fundacjami"), platformy, przedsiębiorstwa zajmujące się analizą danych oraz organy publiczne odpowiedzialne za proces wyborczy. Mają oni obowiązek przetwarzać dane osobowe (na przykład nazwiska i adresy) zgodnie z prawem, rzetelnie oraz w sposób przejrzysty, wyłącznie do określonych celów. Nie mogą one wykorzystywać tych danych w sposób niezgodny z celami, dla których dane zostały pierwotnie zgromadzone. Przetwarzanie danych do celów dziennikarskich również wchodzi w zakres ogólnego rozporządzenia o ochronie danych, ale może korzystać ze zwolnień i odstępstw przewidzianych w prawie krajowym, biorąc pod uwagę znaczenie prawa do wolności wypowiedzi i informacji w społeczeństwie demokratycznym[10].

Pojęcie danych osobowych jest pojęciem bardzo szerokim. „Dane osobowe" to wszelkie dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dane przetwarzane w kontekście wyborczym często obejmują szczególne kategorie danych osobowych („dane wrażliwe"), takie jak poglądy polityczne, przynależność do związków zawodowych, pochodzenie etniczne, seksualność itp., które podlegają większej ochronie[11]. Ponadto w ramach analizy danych z danych niewrażliwych można wydobyć „dane wrażliwe" (takie jak poglądy polityczne, ale również przekonania religijne lub orientacja seksualna). Przetwarzanie tych wydobytych danych również objęte jest zakresem ogólnego rozporządzenia o ochronie danych, w związku z czym powinno ono odbywać się zgodnie z wszystkimi przepisami o ochronie danych.

Dlatego też praktycznie wszystkie operacje przetwarzania danych w kontekście wyborczym podlegają ogólnemu rozporządzeniu o ochronie danych.

Biorąc pod uwagę potrzebę zapewnienia podmiotom zaangażowanym w proces wyborczy klarownych zasad działania oraz uwzględniając pierwsze ustalenia w sprawie Cambridge Analytica, poniżej zaakcentowano obowiązki związane z ochroną danych, których przestrzeganie wydaje się szczególnie istotne w kontekście wyborczym. Ich streszczenie zawarto w załączniku.

2.1 Administratorzy i podmioty przetwarzające

Pojęcie rozliczalności administratorów i współadministratorów danych jest głównym elementem ogólnego rozporządzenia o ochronie danych. Administratorem danych jest podmiot, który decyduje samodzielnie lub we współpracy z innymi, w jakim celu i w jaki sposób dane osobowe są przetwarzane; Podmiot przetwarzający przetwarza dane osobowe wyłącznie w imieniu i pod kierunkiem administratora (na zasadach określonych w umowie lub w innym wiążącym akcie prawnym). Administratorzy danych mają obowiązek

[10] Art. 85 ust. 2 ogólnego rozporządzenia o ochronie danych.
[11] Art. 9 ust. 1 ogólnego rozporządzenia o ochronie danych.

wprowadzić środki odpowiednie do zagrożeń i wdrożyć ochronę danych od samego początku już w fazie projektowania oraz móc wykazać, że przestrzegają ogólnego rozporządzenia o ochronie danych (zasada rozliczalności).

Rolę administratora danych lub podmiotu przetwarzającego należy oceniać w każdym indywidualnym przypadku. W kontekście wyborczym administratorami danych może być szereg podmiotów: partie polityczne, kandydaci indywidualni i fundacje w większości przypadków są administratorami danych; Platformy i przedsiębiorstwa zajmujące się analizą danych mogą być (współ) administratorami lub podmiotami przetwarzającymi w odniesieniu do danego przetwarzania w zależności od stopnia ich kontroli nad danym przetwarzaniem[12]; krajowe organy wyborcze są administratorami danych zawartych w rejestrach wyborczych.

Jeżeli przetwarzanie przez nie danych wiąże się z oferowaniem towarów i usług osobom fizycznym w Unii lub monitorowaniem ich zachowania w Unii, przedsiębiorstwa mające siedzibę poza Unią obowiązane są również przestrzegać ogólnego rozporządzenia o ochronie danych. Dotyczy to szeregu platform i przedsiębiorstw zajmujących się analizą danych.

2.2 Zasady, zgodność przetwarzania z prawem oraz specjalne warunki dotyczące „danych wrażliwych”

Podmioty uczestniczące w wyborach mogą przetwarzać dane osobowe, w tym te uzyskane ze źródeł publicznych, wyłącznie zgodnie z zasadami dotyczącymi przetwarzania danych osobowych oraz w oparciu o zamknięty katalog podstaw wyraźnie określonych w ogólnym rozporządzeniu o ochronie danych[13]. Wydaje się, że najistotniejszymi podstawami dla zgodnego z prawem przetwarzania danych w kontekście wyborczym są zgoda udzielona przez osobę fizyczną, wypełnienie obowiązku prawnego wynikającego z przepisów unijnych lub krajowych, wykonanie zadania w interesie publicznym oraz uzasadniony interes jednego z podmiotów. Podmioty uczestniczące w wyborach mogą jednak powoływać się na uzasadniony interes wyłącznie wtedy, gdy ich interesy nie są nadrzędne wobec interesów lub podstawowych praw i wolności osób, których dane dotyczą.

Ponadto przechowywanie informacji lub uzyskiwanie dostępu do już przechowywanych informacji na urządzeniach końcowych (komputer, smartfon itp.) powinno być zgodne z wymogami dyrektywy o prywatności i łączności elektronicznej dotyczącymi ochrony urządzeń końcowych, co oznacza, że osoba, której dane dotyczą, musiałaby wyrazić zgodę.

Jeżeli podstawą prawną jest zgoda danej osoby, ogólne rozporządzenie o ochronie danych wymaga, aby została ona udzielona w sposób swobodny i świadomy, poprzez wyraźne działanie potwierdzające[14].

[12] W najnowszym orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (sprawa Świadków Jehowy C-25/17, wyrok z dnia 10 lipca 2018 r.) wyjaśniono, że w pewnych okolicznościach administratorem danych może być organizacja, która „wpływa” na gromadzenie i przetwarzanie danych osobowych.
[13] Art. 5 i art. 6 ogólnego rozporządzenia o ochronie danych.
[14] Art. 7 i art. 4 pkt 11) ogólnego rozporządzenia o ochronie danych.

Organy publiczne zaangażowane w proces wyborczy przetwarzają dane osobowe w celu wypełnienia obowiązku prawnego lub wykonania zadania w interesie publicznym. Inne podmioty zaangażowane w proces wyborczy mogą przetwarzać dane na podstawie zgody lub prawnie uzasadnionego interesu[15]. Partie polityczne i fundacje mogą również przetwarzać dane ze względu na interes publiczny, jeżeli tak stanowi prawo krajowe[16].

Organy władzy publicznej mogą ujawniać partiom politycznym niektóre informacje o osobach fizycznych widniejących na listach wyborczych lub w rejestrach mieszkańców, takie jak nazwisko i adres, jedynie wówczas, gdy jest to wyraźnie dopuszczone przez prawo państwa członkowskiego oraz wyłącznie w celu wydawania obwieszczeń wyborczych i w zakresie, w jakim jest to niezbędne do tego celu.

Przetwarzanie danych w kontekście wyborczym często wiąże się z „danymi wrażliwymi". Przetwarzanie takich danych, w tym wydobytych „danych wrażliwych", jest zasadniczo zabronione, chyba że zastosowanie ma jeden z wyjątków, o których mowa w ogólnym rozporządzeniu o ochronie danych[17]. Przetwarzanie „danych wrażliwych" wymaga spełnienia szczególnych, bardziej rygorystycznych warunków: wymaga się, aby dana osoba wyraziła w sposób wyraźny zgodę[18] lub dane te upubliczniła[19]. Partie i fundacje polityczne mogą również przetwarzać „dane wrażliwe", jeżeli zgodnie z prawem Unii lub prawem państwa członkowskiego zachodzi przesłanka ważnego interesu publicznego oraz ustanowiono odpowiednie zabezpieczenia[20]. Ogólne rozporządzenie o ochronie danych stanowi, że podmioty te mogą również przetwarzać „dane wrażliwe" pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tych podmiotów lub osób utrzymujących z nimi stałe kontakty, lecz wyłącznie do celów ujawniania w ramach ich partii politycznej lub fundacji[21]. Ten szczególny przepis nie może być jednak stosowany przez partię polityczną do przetwarzania danych przyszłych jej członków lub wyborców.

Cel przetwarzania danych należy określić w chwili zbierania danych (zasada „ograniczenia celu")[22]. Dane zbierane wyłącznie w jednym celu mogą być dalej przetwarzane tylko w celu, który jest zgodny z pierwotnym celem; w przeciwnym razie należy wskazać nową podstawę prawną przetwarzania, przewidzianą w ogólnym rozporządzeniu o ochronie danych, dla przetwarzania w nowym celu. W szczególności, gdy brokerzy danych na temat stylu życia zbierają dane dla celów handlowych, dane te nie mogą być dalej przetwarzane w kontekście wyborczym.

[15] O ile nie wpływa to istotnie na prawa i wolności osób, których dane dotyczą.
[16] Zob. motyw 56 ogólnego rozporządzenia o ochronie danych „jeżeli w ramach działań związanych z wyborami funkcjonowanie systemu demokratycznego w państwie członkowskim wymaga zbierania przez partie polityczne danych osobowych dotyczących poglądów politycznych obywateli, można zezwolić na przetwarzanie tych danych z uwagi na względy interesu publicznego pod warunkiem ustanowienia odpowiednich zabezpieczeń".
[17] Art. 9 ogólnego rozporządzenia o ochronie danych.
[18] Art. 9 ust. 2 lit. a) ogólnego rozporządzenia o ochronie danych.
[19] Art. 9 ust. 2 lit. e) ogólnego rozporządzenia o ochronie danych.
[20] Art. 9 ust. 2 lit. g) ogólnego rozporządzenia o ochronie danych.
[21] Art. 9 ust. 2 lit. d) ogólnego rozporządzenia o ochronie danych. Partia polityczna lub fundacja nie może udostępniać osobom trzecim danych dotyczących swoich członków lub byłych członków lub osób, które mają z nimi regularny kontakt bez zgody osoby, które dane dotyczą.
[22] Art. 5 ust. 1 lit. b) ogólnego rozporządzenia o ochronie danych.

Partie polityczne i fundacje nie mogą wykorzystywać takich danych uzyskanych od osób trzecich, chyba że dołożą należytej staranności i ustalą, że dane zostały uzyskane zgodnie z prawem.

2.3 Wymogi dotyczące przejrzystości

Sprawa Cambridge Analytica pokazała, jak ważne jest zwalczanie braku transparentności oraz właściwe informowanie osób, których dane dotyczą. Nierzadko osoby fizyczne nie wiedzą, kto przetwarza ich dane osobowe i do jakich celów. Zasady rzetelnego i przejrzystego przetwarzania danych wymagają, by osoby, których dane dotyczą, były informowane o przetwarzaniu i o jego celach[23]. Ogólne rozporządzenie o ochronie danych doprecyzowuje obowiązki administratorów danych w tym zakresie. Mają oni obowiązek informować osoby fizyczne o najważniejszych aspektach związanych z przetwarzaniem ich danych osobowych, takich jak:

- tożsamość administratora,
- cele przetwarzania,
- odbiorcy danych osobowych,
- informacje o źródle danych, jeżeli dane nie pochodzą bezpośrednio od osoby, której dotyczą,
- informacje o zautomatyzowanym podejmowaniu decyzji oraz
- wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania[24].

Ponadto ogólne rozporządzenie o ochronie danych wymaga, aby informacje były podawane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem[25]. Przykładowo krótka, nieprzejrzysta informacja o ochronie danych, zamieszczona w całości drobnym drukiem na materiałach wyborczych, nie spełniłaby wymogów dotyczących przejrzystości.

Zgodnie ze wstępnymi ustaleniami w sprawie Cambridge Analytica niepełne informacje o celu, dla którego zebrano dane stanowiły niedociągnięcie kluczowe w tej sprawie. Poddało ono w wątpliwość ważność zgód udzielonych przez osoby, których dane dotyczyły. Wszelkie podmioty przetwarzające dane osobowe w kontekście wyborczym mają obowiązek upewnić się, że osoby fizyczne w pełni rozumieją, w jaki sposób i w jakim celu ich dane osobowe zostaną wykorzystane, zanim wyrażą na to zgodę lub zanim administrator przystąpi do przetwarzania danych ze względu na każdą inną podstawę przetwarzania.

Osoby fizyczne należy informować na każdym etapie przetwarzania, nie tylko podczas zbierania danych.

[23] Art. 5 ust. 1 lit. a) ogólnego rozporządzenia o ochronie danych.
[24] Art. 13 i art. 14 ogólnego rozporządzenia o ochronie danych.
[25] Wytyczne Europejskiej Rady Ochrony Danych dotyczące przejrzystości.

W szczególności, gdy partie polityczne przetwarzają dane uzyskane od osób trzecich (np. pochodzące z rejestrów wyborczych, od brokerów danych, analityków danych i z innych źródeł), zazwyczaj mają informować i wyjaśniać osobom, których dane dotyczą, w jaki sposób kompilują i wykorzystują te dane w celu zapewnienia rzetelnego przetwarzania[26].

2.4 Profilowanie, zautomatyzowane podejmowanie decyzji oraz mikrotargetowanie

Profilowanie polega na zautomatyzowanym przetwarzaniu danych osobowych wykorzystywanym do analizy lub prognozowania aspektów dotyczących np. osobistych preferencji, zainteresowań, sytuacji ekonomicznej itp.[27] Profilowanie może być wykorzystywane do celów mikrotargetowania osób fizycznych, tj. do analizy danych osobowych (takich jak historia wyszukiwania w internecie) służącej identyfikowaniu określonych zainteresowań danej grupy osób lub konkretnej osoby w celu wywierania wpływu na działania tej grupy lub tej osoby. Mikrotargetowanie może być wykorzystywane w celu zaoferowania spersonalizowanej informacji dla osoby fizycznej lub grupy odbiorców korzystających z usług online, np. z mediów społecznościowych.

Sprawa Cambridge Analytica pokazała, że z mikrotargetowaniem w mediach społecznościowych wiążą się szczególne wyzwania. Podmioty mogą wydobywać dane zebrane dzięki użytkownikom mediów społecznościowych w celu stworzenia profili wyborców. Dzięki temu podmioty takie mogą identyfikować wyborców, na których znacznie łatwiej można wywierać wpływ i tym samym podmioty takie są w stanie wpływać na wynik wyborów.

Do takiego przetwarzania danych stosuje się wszystkie ogólne zasady i przepisy ogólnego rozporządzenia o ochronie danych, takie jak zasady legalności, uczciwości i przejrzystości oraz ograniczenia celu. Osoby fizyczne bardzo często nie są świadome, że są profilowane: nie zdają sobie sprawy, dlaczego otrzymują one jakąś reklamę, która w sposób oczywisty powiązana jest z ich najnowszymi wyszukiwaniami, lub dlaczego otrzymują one spersonalizowane wiadomości od różnych podmiotów. Ogólne rozporządzenie o ochronie danych zobowiązuje wszystkich administratorów danych, na przykład partie polityczne lub analityków danych, do informowania osób fizycznych, w przypadku gdy wykorzystują one takie techniki oraz o skutkach ich stosowania[28].

Ogólne rozporządzenie o ochronie danych stanowi, że zautomatyzowane podejmowanie decyzji, w tym profilowanie, może mieć poważne skutki. Ogólne rozporządzenie o ochronie danych przewiduje, że osoba fizyczna ma prawo do tego, by nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych i wywołującej skutki prawne dotyczące tej osoby lub w podobny sposób znacząco na nią wpływać, chyba że takie przetwarzanie odbywa się na ściśle określonych warunkach, tj. gdy osoby fizyczne udzielają

[26] Art. 14 ogólnego rozporządzenia o ochronie danych.
[27] Art. 4 pkt 4) ogólnego rozporządzenia o ochronie danych.
[28] Art. 13 ust. 2 ogólnego rozporządzenia o ochronie danych.

w sposób wyraźny zgody lub gdy pozwalają na to przepisy prawa Unii lub państwa członkowskiego, które określają odpowiednie środki ochronne[29].

Do tej kategorii należą praktyki mikrotargetowania w celach wyborczych, o ile wywierają wystarczająco znaczący wpływ na osoby fizyczne. Europejska Rada Ochrony Danych stwierdziła, że z taką sytuacją mamy do czynienia, gdy dana decyzja może mieć istotny wpływ na okoliczności, zachowanie lub wybory osób fizycznych lub wywierać dłuższy lub stały wpływ na daną osobę[30]. Rada uznała, że internetowa reklama ukierunkowana może w niektórych przypadkach mieć zdolność do wywierania wystarczająco znaczącego wpływu na osoby fizyczne, na przykład wówczas, gdy jest natrętna lub bazuje na informacjach o tym, na co podatni są jej odbiorcy. Mając na uwadze znaczenie korzystania z demokratycznego prawa do głosowania, spersonalizowane wiadomości, które na przykład mogą wpływać na wyborców w ten sposób, że zaniechają oni pójścia na wybory lub oddadzą oni swój głos w określony sposób, mogą potencjalnie spełniać kryterium znaczącego wpływu.

Administratorzy danych powinni zatem zapewnić, aby jakiekolwiek przetwarzanie w kontekście wyborczym przy zastosowaniu takich technik było legalne, zgodnie z wyżej wymienionymi zasadami oraz ściśle określonymi warunkami ogólnego rozporządzenia o ochronie danych.

2.5 Bezpieczeństwo i prawidłowość danych osobowych

Bezpieczeństwo ma szczególne znaczenie w kontekście wyborczym, biorąc pod uwagę wielkość zbiorów danych oraz fakt, że zbiory te często zawierają „dane wrażliwe". Ogólne rozporządzenie o ochronie danych nakłada na operatorów pracujących z danymi osobowymi (zarówno administratorów, jak i podmioty przetwarzające) obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa odpowiadającego ryzyku związanemu z przetwarzaniem dla praw i wolności osób fizycznych[31].

Ogólne rozporządzenie o ochronie danych nakłada na administratorów wymóg powiadamiania właściwego organu nadzorczego o przypadkach naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później jednak niż w ciągu 72 godzin. Jeżeli dane naruszenie ochrony danych osobowych może spowodować duże zagrożenie dla praw i wolności osób fizycznych, administrator ma również obowiązek bez zbędnej zwłoki poinformować o nim te osoby, których to naruszenie dotyczy[32].

Partie polityczne i inne podmioty zaangażowane w proces wyborczy obowiązane są zwracać szczególną uwagę na to, by zapewniać poprawność danych osobowych w odniesieniu do dużych zbiorów danych oraz przy zbieraniu danych z różnych, niejednorodnych źródeł. Dane

[29] Art. 22 ogólnego rozporządzenia o ochronie danych.
[30] Wytyczne Europejskiej Rady Ochrony Danych dotyczące zautomatyzowanego podejmowania decyzji, WP251rev.01, w wersji zmienionej i przyjętej w dniu 6.02.2018 r.
[31] Art. 32 ogólnego rozporządzenia o ochronie danych.
[32] Art. 33 i art. 34 ogólnego rozporządzenia o ochronie danych. Wytyczne Europejskiej Rady Ochrony Danych dotyczące powiadamiania o naruszeniu ochrony danych osobowych.

niepoprawne należy natychmiast usunąć lub sprostować oraz, w miarę potrzeby, zaktualizować.

2.6 Ocena skutków w zakresie ochrony danych

Ogólne rozporządzenie o ochronie danych wprowadza nowe narzędzie oceny ryzyka przed rozpoczęciem przetwarzania: ocenę skutków dla ochrony danych. Jej przeprowadzenie jest wymagane zawsze, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych[33]. Z taką sytuacją mamy do czynienia w kontekście wyborów, gdy administrator danych systematycznie i wyczerpująco dokonuje oceny czynników osobowych osoby fizycznej (w tym stosuje profilowanie), które istotnie wpływają na daną osobę, oraz gdy administrator przetwarza dane szczególnie wrażliwe na dużą skalę. Krajowe organy wyborcze, które podejmują działania w ramach wykonywania swoich zadań publicznych, mogą nie być zobligowane do przeprowadzenia oceny skutków w zakresie ochrony danych, jeżeli ocena skutków w zakresie ochrony danych została już przeprowadzona w kontekście przyjmowania regulacji prawnych.

Oceny skutków, które mają zostać przeprowadzone przez różne podmioty w kontekście wyborów, powinny obejmować elementy niezbędne do uwzględnienia ryzyka związanego z takim przetwarzaniem, w szczególności zgodność przetwarzania z prawem również w przypadku zestawów danych uzyskanych od stron trzecich oraz wymogi dotyczące przejrzystości.

3. Prawa osób fizycznych

Ogólne rozporządzenie o ochronie danych przyznaje osobom fizycznym dodatkowe i większe prawa, które nabierają szczególnego znaczenia w kontekście wyborów:

- prawo dostępu do swoich danych osobowych;
- prawo do żądania usunięcia swoich danych osobowych, jeżeli przetwarzanie danych odbywa się za zgodą, a zgoda ta została wycofywana, jeżeli dane te nie są już potrzebne lub jeżeli przetwarzanie jest niezgodne z prawem; oraz
- prawo do poprawienia nieprawidłowych lub niekompletnych danych osobowych.

Osoby fizyczne mają również prawo sprzeciwu wobec przetwarzania (na przykład danych zawartych na listach wyborczych przekazanych partiom politycznym), jeżeli przetwarzanie ich danych odbywa się w oparciu o „uzasadniony interes” lub „interes publiczny”.

Osoby fizyczne mają prawo do tego, by nie podlegać decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu ich danych osobowych. W takich przypadkach dana osoba może zażądać ludzkiej interwencji i skorzystać z prawa do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

[33] Art. 35 i art. 36 ogólnego rozporządzenia o ochronie danych. Wytyczne Europejskiej Rady Ochrony Danych dotyczące przeprowadzania oceny w zakresie ochrony danych.

Aby osoby fizyczne mogły korzystać z tych praw, wszystkie zaangażowane podmioty mają obowiązek dostarczyć niezbędnych narzędzi i ustawień. Ogólne rozporządzenie o ochronie danych przewiduje możliwość opracowania kodeksu postępowania zatwierdzonego przez organ ochrony danych, określającego stosowanie w określonych obszarach, w tym w kontekście wyborczym.

Ogólne rozporządzenie o ochronie danych przyznaje osobom fizycznym prawo do wniesienia skargi do organu nadzorczego oraz prawo do środka ochrony prawnej przed sądem. Przyznaje ono również osobom fizycznym prawo do umocowania organizacji pozarządowej do wniesienia skargi w ich imieniu[34]. W niektórych państwach członkowskich przepisy krajowe umożliwiają organizacji pozarządowej złożenie skargi bez uzyskania umocowania od danej osoby. Ma to szczególne znaczenie w kontekście wyborczym, biorąc pod uwagę dużą liczbę osób, których dane dotyczą.

[34] Art. 80 ust. 1 ogólnego rozporządzenia o ochronie danych.

Najważniejsze kwestie związane z ochroną danych, które są istotne w procesie wyborczym[35]

Partie polityczne i fundacje	Partie i fundacje polityczne są administratorami danych.
	• Przestrzegają zasady ograniczenia celu, dalszego przetwarzania wyłącznie do celów zgodnych z celem pierwotnym (np. wymieniając dane z platformami). • Opierają się na właściwej podstawie prawnej przetwarzania (również w odniesieniu do wydobytych danych): zgodzie, uzasadnionym interesie, realizacji zadania w interesie publicznym (jeżeli jest to przewidziane prawem), szczególnych warunkach dotyczących „danych wrażliwych" (np.: poglądy polityczne). • Przeprowadzają ocenę skutków w zakresie ochrony danych. • Informują osoby fizyczne każdorazowo o celu przetwarzania (wymogi dotyczące przejrzystości), zarówno jeżeli chodzi o zbieranie danych bezpośrednio, jak i pozyskiwanie ich od osób trzecich. • Zapewniają, aby dane były prawidłowe, w szczególności dane pochodzące z różnych źródeł oraz dane wydobyte. • Sprawdzają, czy dane uzyskane od osób trzecich zostały uzyskane zgodnie z prawem i do jakich celów (np.: czy osoby, których dane dotyczą, wyraziły w sposób świadomy zgodę na przetwarzanie w danym celu). • Uwzględniają szczególne ryzyko związane z profilowaniem oraz stosują odpowiednie zabezpieczenia. • Przestrzegają szczególnych warunków stosowania zautomatyzowanego podejmowania decyzji (np. uzyskują wyrażoną w sposób wyraźny zgodę i wdrażają właściwe zabezpieczenia). • Jasno identyfikują, kto ma dostęp do danych. • Zapewniają bezpieczeństwo przetwarzania za pomocą środków technicznych i organizacyjnych; zgłaszają naruszenia ochrony danych. • Jasno przedstawiają obowiązki w umowach lub innych aktach prawnie wiążących zawieranych z przetwarzającymi dane, takimi jak przedsiębiorstwa zajmujące się analizą danych. • Usuwają dane, jeżeli dane te nie są już niezbędne do celów,

[35] Powyższe informacje nie są w żadnym razie wyczerpujące. Chodzi tutaj o podkreślenie szeregu kluczowych obowiązków dotyczących danych, które wynikają z ogólnego rozporządzenia o ochronie danych, a które są istotne dla procesu wyborczego. Odnoszą się one do scenariusza, w którym partie polityczne same gromadzą dane (ze źródeł publicznych, ich obecności w mediach społecznościowych, bezpośrednio od wyborców itd.) oraz korzystają z usług brokerów danych lub przedsiębiorstw zajmujących się analizą danych w celu targetowania wyborców za pośrednictwem platform społecznościowych. Platformy mogą również być źródłem danych dla wyżej wymienionych podmiotów Zastosowanie mogą mieć również inne regulacje prawne, takie jak postanowienia dyrektywy o prywatności i łączności elektronicznej dotyczące wysyłania niezamówionych komunikatów i ochrony urządzeń końcowych.

<table>
<tr><td></td><td colspan="2">w których były zbierane.</td></tr>
<tr><td rowspan="3">Brokerzy danych i spółki zajmujące się analizą danych</td><td colspan="2">Platformy i przedsiębiorstwa zajmujące się analizą danych są (współ) administratorami lub podmiotami przetwarzającymi w zależności od stopnia kontroli, jaką sprawują nad danym przetwarzaniem.</td></tr>
<tr><td>Jako administrator danych</td><td>Jako podmioty przetwarzające</td></tr>
<tr><td>• Przestrzegają zasady ograniczenia celu, dalszego przetwarzania wyłącznie do celów zgodnych z celem pierwotnym (w szczególności wymieniając dane z osobami trzecimi).
• Wskazują odpowiednią podstawę prawną przetwarzania: zgodę, uzasadniony interes. Jeżeli mają do czynienia z „danymi wrażliwymi”, przetwarzanie jest możliwe tylko wówczas, gdy zgoda została udzielona w sposób wyraźny lub dane zostały w sposób oczywisty upublicznione.
• Przeprowadzają ocenę skutków w zakresie ochrony danych.
• Informują osoby fizyczne każdorazowo o celu przetwarzania (wymogi dotyczące przejrzystości), w szczególności gdy wymagane jest uzyskanie zgody, ponieważ zazwyczaj dane zostaną sprzedane osobie trzeciej.
• Przestrzegają szczególnych warunków stosowania zautomatyzowanego podejmowania decyzji (np. uzyskują udzieloną w sposób wyraźny zgodę i wdrażają właściwe zabezpieczenia).
• Zwracają szczególną uwagę na to, czy przetwarzanie danych jest zgodne z prawem, oraz czy kompilowane z różnych zestawów dane są prawidłowe.
• Zapewniają bezpieczeństwo przetwarzania za pomocą środków technicznych i organizacyjnych; zgłaszają naruszenia ochrony danych.</td><td>• Przestrzegają obowiązków wynikających z umowy lub innego wiążącego aktu prawnego zawartego z administratorem.
• Zapewniają bezpieczeństwo przetwarzania za pomocą środków technicznych i organizacyjnych.
• Udzielają administratorowi wsparcia w przeprowadzaniu oceny skutków w zakresie ochrony danych lub w wykonywaniu praw przysługujących osobom, których dane dotyczą, lub w celu bezzwłocznego powiadamiania administratora o naruszeniu ochrony danych, jeżeli stwierdzili naruszenie.</td></tr>
</table>

	Platformy są zazwyczaj administratorami danych na nich przetwarzanych oraz ewentualnie współadministratorami wraz z innymi podmiotami.
Platformy społecznościowe/sieci reklamy online	• Wskazują odpowiednią podstawę prawną przetwarzania: umowa z osobą fizyczną, zgoda, uzasadniony interes. Jeżeli mają do czynienia z „danymi wrażliwymi", przetwarzanie jest możliwe tylko wówczas, gdy zgoda została udzielona w sposób wyraźny lub dane zostały w sposób oczywisty upublicznione. • Wykorzystują wyłącznie dane niezbędne do zidentyfikowanego celu. • Przeprowadzają ocenę skutków w zakresie ochrony danych. • Zapewniają zgodność z prawem udostępniania danych ich członków osobom trzecim. • Przestrzegają wymogów dotyczących przejrzystości, w szczególności w odniesieniu do warunków korzystania, jeżeli dane są następnie udostępniane osobie trzeciej itd. • Przestrzegają szczególnych warunków stosowania zautomatyzowanego podejmowania decyzji (np. uzyskują udzieloną w sposób wyraźny zgodę i wdrażają właściwe zabezpieczenia). • Zapewniają bezpieczeństwo przetwarzania za pomocą środków technicznych i organizacyjnych; zgłaszają naruszenia ochrony danych. • Zapewniają, że osoby fizyczne mogą przeprowadzić kontrole i skorzystać z odpowiednich ustawień w celu efektywnego korzystania z przysługujących im praw, w tym z prawa do odmowy poddania się decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.
	Krajowe organy wyborcze są administratorami danych.
Krajowe organy wyborcze	• Podstawa prawna przetwarzania: wypełnienie obowiązku prawnego lub wykonanie zadania realizowanego w interesie publicznym wynikającego z przepisów prawa. • Przeprowadzenie oceny skutków w zakresie ochrony danych, jeżeli ocena skutków nie została już przeprowadzona w ramach przyjmowania regulacji prawnych.