

Poradnik

„Ochrona danych osobowych w trakcie prowadzenia kampanii wyborczej”

Zestaw wytycznych dla komitetów wyborczych, partii politycznych, kandydatów, wyborców oraz stowarzyszeń i organizacji społecznych, jak zorganizować kampanię wyborczą z poszanowaniem przepisów o ochronie danych osobowych i prawa do prywatności.

Wprowadzenie

Wybory powszechne są niezbędnym warunkiem właściwego funkcjonowania współczesnych demokracji, dając obywatelom możliwość udziału w życiu publicznym i wpływu na kształt polityki państwa na jego różnych szczeblach.

Zgłaszanie kandydatów w wyborach oraz prowadzenie na ich rzecz kampanii wyborczej należy do komitetów wyborczych, które w zależności od rodzaju wyborów mogą być tworzone przez różne podmioty (partie polityczne lub ich koalicje, wyborców, czy stowarzyszenia i organizacje społeczne). Wśród tych podmiotów największą rolę odgrywają partie polityczne, czyli organizacje mające na celu wywieranie metodami demokratycznymi wpływu na kształtowanie polityki państwa lub sprawowanie władzy publicznej i to nie tylko w okresie kampanii wyborczej. Podkreślenia wymaga, że w państwach demokratycznych jedną z podstawowych wartości konstytucyjnych jest wolność tworzenia partii politycznych. Cele i zasady działania partii politycznych nie mogą naruszać Konstytucji Rzeczypospolitej Polskiej (Dz. U. Nr 78, poz. 483 z późn. zm.), a także przepisów ustawy z dnia 27 czerwca 1997 r. o partiach politycznych (Dz. U. z 2011 r. Nr 155, poz. 924 z późn. zm.).

W systemie demokratycznym władza jest zdobywana dzięki wygranym wyborom. Dlatego nie dziwi, że zabiegi zmierzające do pozyskania poparcia wyborców w okresie kampanii wyborczej podlegają szczególnej intensyfikacji. Te działania często wiążą się z wykorzystywaniem danych osobowych i podlegają rygorom określonym przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.), zwaną dalej ustawą lub ustawą o ochronie danych osobowych. Należy bowiem pamiętać, że komitety wyborcze oraz inne podmioty zaangażowane w kampanię wyborczą muszą przestrzegać nie tylko przepisów bezpośrednio regulujących jej przebieg, ale również przepisów ustawy o ochronie danych osobowych. Ma to tym większe znaczenie, że przepisy regulujące przebieg wyborów w ograniczonym zakresie odnoszą się do kwestii związanych z ochroną danych osobowych. W demokratycznym państwie prawnym, osoby sprawujące

funkcje publiczne, w szczególności pochodzące z wyboru bądź kandydujące na te stanowiska, powinny zwracać szczególną uwagę na to, aby ich działania nie naruszały przepisów obowiązującego prawa.

Biorąc pod uwagę liczne sygnały dotyczące nieprawidłowości związanych z przetwarzaniem danych osobowych w trakcie dotychczasowych kampanii wyborczych, niniejszy poradnik ma pomóc w zapobieżeniu dalszego ich występowania.

I. AKTY PRAWA REGULUJĄCE PRZEBIEG WYBORÓW

Dotychczas problematyka przeprowadzania wyborów określona była w licznych szczególnych aktach prawnych. Wśród nich wymienić należy:

- ustawę z dnia 12 kwietnia 2001 r. Ordynacja wyborcza do Sejmu Rzeczypospolitej Polskiej i do Senatu Rzeczypospolitej Polskiej (Dz. U. z 2007 r. Nr 190, poz. 1360 z późn. zm.),
- ustawę z dnia 27 września 1990 r. o wyborze Prezydenta Rzeczypospolitej Polskiej (Dz. U. z 2010 r. Nr 72, poz. 467),
- ustawę z dnia 16 lipca 1998 r. Ordynacja wyborcza do rad gmin, rad powiatów i sejmików województw (Dz. U. z 2010 r. Nr 176, poz. 1190 z późn. zm.),
- ustawę z dnia 20 czerwca 2002 r. o bezpośrednim wyborze wójta, burmistrza i prezydenta miasta (Dz. U. z 2010 Nr 176, poz. 1191),
- ustawę z dnia 23 stycznia 2004 r. Ordynacja wyborcza do Parlamentu Europejskiego. (Dz. U. z 2004 r. Nr 25, poz. 219 z późn. zm.)
- akty wykonawcze wydane na podstawie wymienionych ustaw.

W dniu 1 sierpnia 2011 r. weszła w życie ustawa **z dnia 5 stycznia 2011 r. - Kodeks wyborczy** (Dz. U. Nr 21, poz. 112 z późn. zm.), która w sposób kompleksowy uregulowała zasady i tryb zgłaszania kandydatów oraz przeprowadzania wyborów na Prezydenta RP, do Sejmu i Senatu RP, do Parlamentu Europejskiego, a także do organów stanowiących jednostek samorządu terytorialnego oraz wójtów, burmistrzów i prezydentów miast.

Jednakże w Kodeksie wyborczym o wiele łatwiej jest wskazać zakazy odnoszące się do przebiegu kampanii wyborczej niż określić nakazy jej dotyczące, w szczególności w obszarze przetwarzania danych osobowych. W konsekwencji, w razie braku w tym zakresie szczególnych przepisów w Kodeksie wyborczym lub innych aktach prawnych regulujących przeprowadzanie wyborów, należy stosować przepisy ustawy o ochronie danych osobowych.

II. PODSTAWOWE POJĘCIA I ZASADY OCHRONY DANYCH OSOBOWYCH

1. Źródła prawa ochrony danych osobowych

Prawo do ochrony danych osobowych jest prawem człowieka, zagwarantowanym w art. 51 Konstytucji Rzeczypospolitej Polskiej, które zostało rozwinięte w ustawie o ochronie danych osobowych. Ustawa ta określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.

2. Dane osobowe

Danymi osobowymi są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, pozwalające bez większego wysiłku na określenie tożsamości tej osoby.

Możliwa do zidentyfikowania jest taka osoba, której tożsamość można określić bezpośrednio lub pośrednio, zwłaszcza poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Ustawa przewiduje dwie kategorie danych osobowych:

- a) tzw. dane zwykłe (np. imię, nazwisko, adres zamieszkania, wykonywany zawód, numer telefonu, itp.);
- b) dane szczególnie chronione – sensytywne, wymienione enumeratywnie w art. 27 ust. 1 ustawy, dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów, życia seksualnego, skazań, orzeczeń o ukaraniu i mandatów karnych, innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

3. Zbiór danych

Zgodnie z art. 7 pkt 1 ustawy zbiorem danych jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Zatem zbiorem danych

jest zestaw informacji charakteryzujących się następującymi cechami:

- a) jest to zestaw danych osobowych, tj. informacji o charakterze osobowym;
- b) posiadający ustaloną strukturę, tj. taki, w którym dane są uporządkowane i ułożone w odpowiedni sposób;
- c) dane w nim zawarte są dostępne według określonych kryteriów, co oznacza, że istnieje pewien klucz ich wyszukiwania w zbiorze, pozwalający na w miarę szybkie i bezpośrednie odszukanie interesujących danych osobowych, bez konieczności przeglądania całego zbioru lub znacznej jego części; nie ma przy tym znaczenia liczba ani rodzaje kryteriów - może to być zarówno kryterium osobowe (np. imię, nazwisko, data urodzenia, PESEL) lub nieosobowe (np. data zamieszczenia danych w zbiorze, liczba porządkowa).

Pojęcie zbioru danych obejmuje swym zakresem zarówno zbiory zautomatyzowane, przetwarzane przy użyciu aplikacji bazujących na systemach zarządzających bazami danych, jak i niezautomatyzowane (manualne, tradycyjne). Zbiorami danych mogą być więc np. ręcznie tworzone zbiory ewidencyjne, zgromadzone akta osobowe (teczki, kartoteki), a także formularze czy kwestionariusze, uporządkowane i ułożone w odpowiedni sposób.

4. Przetwarzanie danych

Przetwarzaniem danych są jakiegokolwiek czynności na danych osobowych, w szczególności: zbieranie, utrwalanie, opracowywanie, zmienianie, udostępnianie, usuwanie, przechowywanie (archiwizowanie), operacje wykonywane w systemach informatycznych.

Każda operacja przetwarzania danych osobowych wymaga wykazania odpowiedniej podstawy prawnej.

5. Podstawy prawne przetwarzania danych osobowych

Przetwarzanie danych zwykłych odbywa się na podstawie art. 23 ust. 1 ustawy, i jest dopuszczalne tylko wtedy, gdy:

- a) osoba, której dane dotyczą, wyrazi na to zgodę;
- b) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- c) jest konieczne dla realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy;
- d) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

e) jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

Każda z tych przesłanek jest autonomiczna i może stanowić samodzielną podstawę przetwarzania danych osobowych.

Przetwarzanie danych szczególnie chronionych, co do zasady jest zabronione, za wyjątkiem sytuacji określonych w art. 27 ust. 2 ustawy, np. gdy jest to niezbędne do wykonania statutowych zadań instytucji o celach politycznych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych (art. 27 ust. 2 pkt 4). Przetwarzanie danych szczególnie chronionych jest także dopuszczalne za pisemną zgodą osób, których dane dotyczą (art. 27 ust. 2 pkt 1 ustawy).

6. Zgoda

W myśl art. 7 pkt 5 ustawy o ochronie danych osobowych, przez zgodę osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda składającego oświadczenie na przetwarzanie jego danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie. Z definicji tej nie wynikają szczegółowe zasady formułowania klauzul zgody, jednakże podkreśla się, że z treści klauzul zgody na przetwarzanie danych osobowych powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi. W przypadku zgody na wykorzystywanie danych osobowych podlegających szczególnej ochronie – zgoda musi być wyrażona na piśmie.

7. Administrator danych

Administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych (art. 7 pkt 4 ustawy). Między innymi może to być: organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna. Administratorem danych będzie więc komitet wyborczy, partia polityczna, czy poseł lub senator w zakresie ustawowo realizowanych zadań.

8. Podstawowe obowiązki administratora danych

Przepisy ustawy o ochronie danych osobowych nakładają na administratora danych określone obowiązki. Zgodnie z art. 26 ust. 1 ustawy, ma on dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, jest zobowiązany do przestrzegania następujących zasad:

- a) legalności – dane mają być przetwarzane zgodnie z przepisami prawa, w szczególności po spełnieniu jednej z przesłanek wymienionych w art. 23 ust. 1 lub art. 27 ust 2 ustawy;
- b) celowości – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z tymi celami - przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych (art. 26 ust. 2 ustawy), z zachowaniem przepisów dotyczących dopuszczalności przetwarzania danych (art. 23) i spełnieniem obowiązku informacyjnego w przypadku zbierania danych nie od osoby, której dotyczą (art. 25);
- c) merytorycznej poprawności – dane powinny być merytorycznie poprawne i aktualne;
- d) adekwatności – dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane, tj. ich zakres nie może wykraczać poza to, co jest niezbędne do osiągnięcia tych celów, dane nie mogą być zbierane „na zapas”;
- e) ograniczenia czasowego – dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie mogą być przetwarzane dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Administrator danych jest jednocześnie zobowiązany do:

- a) spełnienia wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 (gdy dane są zbierane bezpośrednio od tych osób) lub w art. 25 ustawy (gdy dane są zbierane z innych źródeł);
- b) zabezpieczenia danych osobowych poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, tak aby: nie były udostępniane osobom nieupoważnionym, zabrane przez osobę nieuprawnioną, a także były zabezpieczone przed uszkodzeniem, zniszczeniem lub utratą;
- c) zgłoszenia zbioru (zbiorów) danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 pkt 1 – 11 ustawy (z obowiązku rejestracji zwolnione są zbiory danych osobowych tworzone między innymi na podstawie przepisów dotyczących wyborów do Sejmu,

Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego, a także prowadzone przez partie polityczne czy stowarzyszenia, zbiory danych osób zrzeszonych w tych partiach, co oznacza, że do rejestracji nie trzeba zgłaszać zbiorów tworzonych na podstawie wymienionych wyżej przepisów, o ile dane osobowe w nich zgromadzone przetwarzane są wyłącznie w określonych w nich celach);

- d) respektowania praw osób, których dane dotyczą, do kontroli przetwarzania ich danych w trybie i na zasadach określonych w rozdziale 4 ustawy pt. „Prawa osoby, której dane dotyczą” (osoby te, do których również należą wyborcy, mogą np. domagać się uzyskania informacji określonych w art. 32 ust. 1 pkt 1-5a ustawy, m.in. czy zbiór danych istnieje, ustalenia administratora danych i adresu jego siedziby, uzyskania informacji o celu, zakresie i sposobie przetwarzania danych oraz informacji o czasie przetwarzania i źródle, z którego pochodzą, sposobie udostępniania danych innym odbiorcom, a także mają prawo żądania uzupełnienia, uaktualnienia, sprostowania, a nawet czasowego lub stałego wstrzymania przetwarzania danych, jeżeli są one nieaktualne, niekompletne, nieprawdziwe lub zostały zebrane z naruszeniem prawa albo są już zbędne do realizacji celu, dla którego były zebrane).

Osoby te mają prawo do sprzeciwu wobec przetwarzania danych w celach marketingowych lub przekazania ich innemu administratorowi, gdy odbywa się to w celu wykonania określonych prawem zadań realizowanych dla dobra publicznego lub dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

Stosownie do art. 35 ust. 1 ustawy, w razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

9. Organ ochrony danych osobowych

Nad przestrzeganiem prawa obywateli do ochrony ich danych osobowych czuwa

niezależny organ – Generalny Inspektor Ochrony Danych Osobowych [dalej też: Generalny Inspektor]. Postępowanie w sprawach uregulowanych w ustawie o ochronie danych osobowych prowadzi się według zasad określonych w przepisach ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2013 r. poz. 267 z późn. zm.), o ile przepisy ustawy o ochronie danych osobowych nie stanowią inaczej (art. 22 ustawy).

Zgodnie z brzmieniem art. 12 ustawy, Generalny Inspektor w szczególności kontroluje zgodność przetwarzania danych z przepisami o ochronie danych osobowych, wydaje decyzje administracyjne i rozpatruje skargi w sprawach wykonania przepisów o ochronie danych osobowych, zapewnia wykonanie przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji, przez stosowanie przewidzianych przepisami prawa środków egzekucyjnych, prowadzi ogólnokrajowy, jawny rejestr zbiorów danych oraz rejestr administratorów bezpieczeństwa informacji, a także udziela informacji o zarejestrowanych zbiorach i zarejestrowanych administratorach bezpieczeństwa informacji, opiniuje projekty ustaw i rozporządzeń dotyczących ochrony danych osobowych, inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych, a także uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor nakazuje, w drodze decyzji administracyjnej, przywrócić stan zgodny z prawem poprzez usunięcie uchybień, uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych, zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe, wstrzymanie przekazywania danych osobowych do państwa trzeciego, zabezpieczenie danych lub przekazanie ich innym podmiotom albo też ich usunięcie. Podkreślenia wymaga fakt, że decyzje Generalnego Inspektora nie mogą ograniczać swobody działania podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta Rzeczypospolitej Polskiej, do Sejmu, do Senatu i do organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem zarządzenia wyborów a dniem głosowania (art. 18 ust. 2 ustawy).

Należy jednak pamiętać, że dla kontroli procesów przetwarzania danych osobowych w związku z wyborami, przepisy prawa mogą wyznaczać inne właściwe podmioty, których orzeczenia podlegają ocenom w toku instancji czy w inny sposób określony odpowiednimi procedurami.

III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W CELACH MARKETINGU WYBORCZEGO

Agitacja wyborcza jest niezbędnym elementem kampanii wyborczej. Art. 105 § 1 Kodeksu wyborczego definiuje ją jako publiczne nakłanianie, zachęcanie do głosowania w określony sposób lub do głosowania na kandydata określonego komitetu wyborczego. Ustawodawca ponadto wskazuje, że każdy wyborca może prowadzić agitację wyborczą na rzecz kandydatów, w tym zbierać podpisy popierające zgłoszenia kandydatów, po uzyskaniu pisemnej zgody pełnomocnika wyborczego. Niewątpliwie agitacja wyborcza może również przybrać formę marketingu bezpośredniego.

Ustawa, choć posługuje się pojęciem marketingu bezpośredniego, to jednak go nie definiuje. Dlatego można się posłużyć definicją zawartą w art. 1 rekomendacji R(85)20 Komitetu Ministrów Rady Europy. Zgodnie z tym przepisem, przez „marketing bezpośredni” należy rozumieć „ogół działań, a także wszelkich dotyczących go usług pomocniczych umożliwiających oferowanie produktów i usług, bądź przekazywanie innych informacji do grupy ludności – za pośrednictwem poczty, telefonu lub innych bezpośrednich środków – w celach informacyjnych bądź w celu wywołania reakcji ze strony osoby, której dane dotyczą”.

Wyraźnie więc widać, że marketing bezpośredni obejmuje nie tylko ofertę produktów lub usług, ale także promocję celów i idei określonych organizacji, w tym partii politycznych czy komitetów wyborczych. Jedną z częściej wykorzystywanych form marketingu bezpośredniego są przesyłki pocztowe zawierające przekazy promocyjne. Przesyłki takie mogą być bezadresowe lub adresowe. W wypadku **przesyłek bezadresowych** na rozpowszechnianych materiałach nie umieszcza się adresu odbiorcy. Takie przesyłki są dostarczane wszystkim osobom zamieszkującym wybrany przez nadawcę obszar. Ze względu na to, że przesyłki bezadresowe nie są kierowane do oznaczonego adresata, a więc nie zawierają danych osobowych, ustawa o ochronie danych osobowych nie będzie miała do nich zastosowania. Z kolei **przesyłki adresowe** są dostarczane ściśle wyselekcjonowanej grupie zindywidualizowanych odbiorców (wyborców), a zatem wiąże się to z przetwarzaniem danych osobowych i musi być zgodne z zasadami ochrony danych osobowych. Każdy administrator danych – w tym każdy komitet wyborczy – o ile gromadzi informacje wyczerpujące definicję danych osobowych, powinien przestrzegać zasad wynikających zarówno z powołanych przepisów szczególnych, jak i ustawy o ochronie danych osobowych.

Komitety wyborcze przetwarzające dane osobowe na potrzeby kampanii wyborczej są

obowiązane legitymować się odpowiednią przesłanką przetwarzania, o której mowa w art. 23 i art. 27 ustawy. W odniesieniu do danych zwykłych ich przetwarzanie jest dopuszczalne, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy). Dla przykładu, komitety wyborcze zgodnie z art. 209 Kodeksu wyborczego tworzą wykazy podpisów poparcia list kandydatów. I co ważne - precyzyjnie określają katalog danych osobowych, jakie mają być ujęte na listach poparcia kandydatów, stanowiąc, iż wyborca udzielający poparcia liście kandydatów składa podpis obok czytelnie wpisanego swojego nazwiska i imienia, adresu zamieszkania i numeru ewidencyjnego PESEL. Przetwarzanie danych osobowych może się również odbywać na podstawie zgody osoby, której dane dotyczą, chyba że chodzi o usunięcie dotyczących jej danych (art. 23 ust. 1 pkt 1 ustawy).

W pewnych okolicznościach przetwarzanie danych na potrzeby marketingu wyborczego może się odbywać zgodnie z art. 23 ust. 1 pkt 5 ustawy, tj. gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą (art. 23 ust. 1 pkt 5 ustawy). Na tę przesłankę w szczególności można się powołać w sytuacji pozyskania danych potencjalnych wyborców ze źródeł powszechnie dostępnych, jak książki telefoniczne. Należy zauważyć, że ma ona zastosowanie jedynie do danych, które stały się powszechnie dostępne zgodnie z prawem. Podkreślenia także wymaga, że w tym wypadku szczególnego znaczenia nabiera konieczność spełnienia w odpowiedni sposób obowiązku informacyjnego. Jakkolwiek należy mocno podkreślić, że co do zasady dane dotyczące wyborców powinny być pozyskiwane albo na podstawie uprawniających do tego przepisów prawa, albo za ich wiedzą i zgodą.

Wielu administratorów danych nie ma świadomości, że naruszają oni ustawę o ochronie danych osobowych. Wychodząc z założenia, że raz zebrane dane stają się ich własnością, zmieniają cel przetwarzania danych, np. dane zebrane w celu zawarcia lub wywiązania się z umowy, są wykorzystywane w innym niż pierwotnie celu. Zgodnie z art. 26 ust. 1 pkt 2 ustawy, administrator przetwarzający dane powinien dołożyć należytej staranności w celu ochrony osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby były one zbierane dla oznaczonych zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Powyższe wiąże się również z koniecznością pozyskiwania danych do celów agitacji wyborczej ze źródeł, z których takie pozyskanie jest zgodne z prawem. Należy również pamiętać m.in. o poinformowaniu zainteresowanych osób o rzeczywistym źródle pozyskania danych osobowych do celów agitacji wyborczej. Komitet

wyborczy musi mieć pewność co do źródła oraz legalności pozyskania z niego danych.

Z tego względu w pierwszej kolejności należy rekomendować zbieranie danych bezpośrednio od osób, których one dotyczą. W przypadku pozyskania danych z innych źródeł, albo ich wykorzystania w sytuacji, gdy pierwotnie zostały zebrane w innym celu, wymaga się szczególnej ostrożności i w wielu sytuacjach nie jest to zgodne z prawem. W szczególności fakt pełnienia przez kandydata funkcji publicznej nie uzasadnia możliwości pozyskania i dalszego przetwarzania danych pochodzących ze zbiorów prowadzonych przez instytucję, w której ta funkcja jest pełniona. W konsekwencji bez uprzedniej zgody osób, których dane dotyczą, nie jest dopuszczalne wykorzystanie ich danych w celach marketingu wyborczego ze zbiorów ewidencji ludności prowadzonej przez gminy lub archiwalnych danych osób, którym poseł lub senator udzielił wsparcia. Ponadto poważnym naruszeniem przepisów o ochronie danych osobowych jest wykorzystanie w celach wyborczych przez różne osoby (czasami członków rodziny kandydata lub jego sympatyków) danych z różnych zbiorów, do których mają one dostęp w ramach wykonywanej przez siebie pracy, np. danych pełnoletnich uczniów szkoły czy danych użytkowników karty miejskiej. Wyraźnie należy zaznaczyć, że takie działanie oznacza udostępnienie danych osobom nieupoważnionym, a komitety wyborcze nie są uprawnione do wykorzystywania tak pozyskanych informacji.

Każdy administrator danych, w tym komitet wyborczy, zbierając dane jest obowiązany spełnić obowiązek informacyjny zarówno wtedy, gdy dane są zbierane bezpośrednio od osób, których one dotyczą, jak i z innych źródeł. Podkreślenia wymaga, że realizacja tego obowiązku ma wielkie znaczenie dla umożliwienia osobom, których dane dotyczą, realizacji swoich praw.

Zgodnie z art. 24 ust. 1 ustawy, **w przypadku zbierania danych osobowych od osoby** której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
- celu zbierania danych, a w szczególności o znanym mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
- prawie dostępu do treści swoich danych oraz ich poprawiania;
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Natomiast w myśl art. 25 ust. 1 ustawy, **w przypadku zbierania danych osobowych nie od osoby, której one dotyczą**, tylko od innych podmiotów, administrator danych jest

obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
- celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
- źródle danych;
- prawie dostępu do treści swoich danych oraz ich poprawiania;
- uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

Warto dodać, że kwestia pozyskiwania danych osobowych od innych podmiotów w kontekście działalności gospodarczej, np. w drodze zakupu, była przedmiotem rozstrzygnięć sądów administracyjnych. I tak, Naczelny Sąd Administracyjny w wyroku z 13 lipca 2004 r. (sygn. akt OSKI 507/2004) stwierdził, że „jeżeli jedna firma kupiła dane osobowe od innej, musi o tym niezwłocznie poinformować osoby, których dotyczy transakcja. Nie wolno też wysyłać jednocześnie ofert marketingowych, gdyż dalsze korzystanie z takich danych zależy od zainteresowanych, którzy mogą zgłosić sprzeciw lub skorzystać z innych form kontroli”.

W tym kontekście należy zwrócić uwagę, że ustawa o ochronie danych osobowych przewiduje wyjątki, w których administrator danych zwolniony jest z dopełnienia obowiązku informacyjnego wynikającego z obu wymienionych wcześniej przepisów. I tak, zgodnie z art. 24 ust. 2 ustawy obowiązek ten nie ma zastosowania, jeżeli:

- przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;
- osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Natomiast na mocy art. 25 ust. 2 ustawy, obowiązku informacyjnego nie stosuje się, jeżeli:

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
- dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;
- dane są przetwarzane przez administratora, będącego organem administracji państwowej, organem samorządu terytorialnego, państwową lub komunalną jednostką organizacyjną

lub podmiotem niepublicznym realizującym zadania publiczne na podstawie przepisów prawa;

- osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Często pojawia się również problem związany z ustaleniem okresu przechowywania danych pozyskanych na potrzeby prowadzenia kampanii wyborczej. Należy jeszcze raz zaznaczyć, że zgodnie z zasadą ograniczenia czasowego dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie mogą być przetwarzane dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania, czyli celu, dla którego zostały zebrane. Oznacza to, że dłuższe przechowywanie danych jest dopuszczalne jedynie w sytuacji, gdy wymagają tego przepisy szczególne.

IV. ZABEZPIECZANIE DANYCH OSOBOWYCH PRZETWARZANYCH NA POTRZEBY KAMPANII WYBORCZEJ

Ustawa o ochronie danych osobowych w rozdziale 5 reguluje podstawowe kwestie dotyczące zabezpieczania danych osobowych. Zgodnie z art. 36 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych. W oparciu zaś o art. 36a ustawy, może powołać administratora bezpieczeństwa informacji, do którego zadań należy m.in. zapewnienie przestrzegania przepisów o ochronie danych osobowych, a także prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.

Ustawa przewiduje również (art. 37), że do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Obowiązek ten ma zastosowanie również osób, które przetwarzają dane osobowe w ramach wolontariatu – na przykład wyborców zbierających listy poparcia kandydatów. Ponadto – zgodnie z art. 38 – administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Ten ostatni wymóg odnosi się nie tylko do kwestii bezpieczeństwa, ale

również funkcjonalności systemu, w którym będą przetwarzane dane osobowe. Funkcjonalność ta musi bowiem zapewniać administratorowi nie tylko bezpieczeństwo danych, ale również możliwość realizacji zobowiązań wobec podmiotów danych, w tym wyborców.

Wśród obowiązków administratora danych związanych z bezpieczeństwem należy wymienić także prowadzenie ewidencji osób upoważnionych do ich przetwarzania, która – zgodnie z art. 39 ust. 1 – powinna zawierać: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych; identyfikator, jeżeli dane są przetwarzane w systemie informatycznym. Ponadto ustawa (art. 39 ust. 2) zobowiązuje osoby, które zostały upoważnione do przetwarzania danych, do zachowania w tajemnicy zarówno tych danych, jak i sposobów ich zabezpieczenia. Ważne jest, że osoba upoważniona do przetwarzania danych nie może wykorzystywać ich na swoją rzecz i w innych celach. Dla przykładu, wolontariusz zbierający listy poparcia kandydatów nie może tak pozyskanych danych wykorzystać w ramach prowadzonej na swoją rzecz innej kampanii wyborczej.

Kwestie związane z właściwą ochroną danych osobowych reguluje również rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwane dalej rozporządzeniem. Zgodnie z § 3-5 rozporządzenia, administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Pojęcie polityki bezpieczeństwa użyte w rozporządzeniu należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych. Polityka bezpieczeństwa swym zakresem powinna obejmować przetwarzanie danych zarówno w systemach informatycznych, jak i w formie tradycyjnej. Jej celem jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

Prawidłowe zarządzanie zasobami, w tym również informacjami, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów oraz określenia miejsca i sposobu ich przetwarzania. Wybór odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją, zależy od zastosowanych nośników informacji, rodzajów urządzeń, sprzętu komputerowego i oprogramowania. Dlatego

w § 4 rozporządzenia wskazano, że polityka bezpieczeństwa powinna zawierać w szczególności:

- wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych;
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- sposób przepływu danych pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych, niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Jednym z wymogów nałożonych na administratorów danych, zgodnie z § 3 ust. 1 rozporządzenia, jest również opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwanej dalej instrukcją. Powinna być ona zatwierdzona przez administratora danych i przyjęta do stosowania jako obowiązujący dokument. Zawarte w niej procedury i wytyczne powinny być przekazywane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności. Na przykład zasady i procedury nadawania uprawnień do przetwarzania danych osobowych czy też sposób prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, powinny być przekazane osobom zarządzającym organizacją przetwarzania danych; sposób rozpoczęcia i zakończenia pracy, sposób użytkowania systemu czy też zasady zmiany haseł – wszystkim osobom będącym jego użytkownikami; zasady ochrony antywirusowej, a także procedury wykonywania kopii zapasowych – osobom zajmującym się techniczną eksploatacją i utrzymaniem ciągłości pracy systemu.

W treści instrukcji powinny być zawarte ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, zastosowanych rozwiązaniach technicznych, jak również procedurach eksploatacji i zasadach użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Gdy administrator do przetwarzania danych wykorzystuje nie jeden, lecz kilka systemów informatycznych, wówczas – stosownie do podobieństwa zastosowanych rozwiązań – powinien opracować jedną, ogólną instrukcję zarządzania lub oddzielne instrukcje dla każdego z użytkowanych systemów. Zatem inny będzie zakres opracowanych

zagadnień w małych podmiotach, w których dane osobowe przetwarzane są przy pomocy jednego lub kilku komputerów, a inny w dużych, w których funkcjonują rozbudowane lokalne sieci komputerowe z dużą liczbą serwerów i stacji roboczych przetwarzających dane przy użyciu wielu systemów informatycznych. W instrukcji powinny być wskazane systemy informatyczne, ich lokalizacje i stosowane metody dostępu (bezpośrednio z komputera, na którym system jest zainstalowany, w lokalnej sieci komputerowej czy też poprzez sieć telekomunikacyjną, np. łącze dzierżawione, Internet).

W odniesieniu do systemów informatycznych ustawa wprowadziła wiele przepisów dotyczących zarówno ich bezpieczeństwa, jak i funkcjonalności. Celem tych regulacji jest zapewnienie, aby systemy informatyczne, używane do przetwarzania danych osobowych, posiadały takie funkcje i mechanizmy, które będą wspomagały administratora w wywiązywaniu się z nałożonych na niego obowiązków. Wymagania te można podzielić najogólniej na dwie grupy. Pierwsza – to wymagania mające na celu zapewnienie ścisłej kontroli nad przetwarzanymi danymi, natomiast druga – to wymagania wynikające z uprawnień osób, których dane są przetwarzane.

Należy podkreślić, iż prawidłowe zabezpieczenie zbiorów danych osobowych wiąże się z koniecznością podjęcia środków, które uniemożliwią dostęp do danych osobom nieupoważnionym. Tytułem przykładu – i co bardzo istotne – zbierając podpisy na listach poparcia poprzez proste przesłonięcie danych osobowych osób, które już wpisały się na te listy tak, by zapewnione zostało nieudostępnianie już zebranych danych osobowych kolejnym osobom, które dokonują wpisu.

V. REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH

Stosownie do art. 40 ustawy o ochronie danych osobowych, administrator danych jest zobowiązany zgłosić zbiór danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, chyba że zachodzi jedna z przesłanek zwalniających go z tego obowiązku, określonych w art. 43 ust. 1 tejże ustawy. Obowiązek zgłoszenia zbioru do rejestracji ciąży zatem na administratorze danych, tj. podmiocie decydującym o celach i środkach przetwarzania (art. 7 pkt 4 ustawy). Status administratora danych może przysługiwać zarówno podmiotom publicznym, jak i prywatnym. Administratorem danych może być zatem np. organ państwowy, organ samorządu terytorialnego, spółka prawa handlowego, stowarzyszenie, partia polityczna, poseł, senator. Ponadto należy wskazać, że

administratorem danych przetwarzanych w jednostce organizacyjnej osoby prawnej jest - co do zasady - dana osoba prawna, a nie jej jednostka organizacyjna.

Przedmiotem zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych jest zbiór danych osobowych. Zgłoszenia zbioru danych należy dokonać przed rozpoczęciem ich przetwarzania. Zgodnie bowiem z art. 46 pkt 1 ustawy administrator danych może rozpocząć ich przetwarzanie po zgłoszeniu tego zbioru do rejestracji. Jednakże, gdy administrator zamierza przetwarzać dane szczególnie chronione, wskazane w art. 27 ustawy, to ich zbieranie może rozpocząć dopiero po zarejestrowaniu zbioru.

Zgłoszenie zbioru danych do rejestracji jest zasadą, od której wyjątki wymienione zostały w art. 43 ust. 1 pkt 1-12 i ust. 1a ustawy o ochronie danych osobowych. Katalog tych wyjątków jest zamknięty i nie może być interpretowany rozszerzająco. W każdym przypadku przetwarzania danych osobowych, administrator jest tą osobą, która dokonuje oceny, czy ze względu na charakter przetwarzanych danych, ich zbiór podlega obowiązkowi zgłoszenia do rejestracji, czy też nie. W tym miejscu należy podkreślić, że zwolnienie zbioru danych z rejestracji jest możliwe tylko wówczas, gdy wskazana w art. 43 ust. 1 ustawy przesłanka dotyczy wszystkich danych zawartych w zbiorze. Jeżeli zatem w ramach określonego zbioru przetwarzane są, choćby incydentalnie, dane inne niż te, wymienione w art. 43 ust. 1 ustawy, bądź w innym celu, niż wskazany w tym przepisie, to zbiór podlega obowiązkowi zgłoszenia do rejestracji.

Biorąc pod uwagę adresatów niniejszego poradnika należy zwrócić uwagę przede wszystkim na dwie z przesłanek zwolnienia z obowiązku rejestracji zbioru.

Pierwszą jest art. 43 ust. 1 pkt 4 ustawy, który stanowi, iż z obowiązku rejestracji zbioru danych zwolnieni są m.in. administratorzy danych dotyczących osób u nich zrzeszonych. Partia polityczna, zgodnie z art. 1 i 3 ustawy o partiach politycznych, jest dobrowolną organizacją, stawiającą sobie za cel udział w życiu publicznym poprzez wywieranie metodami demokratycznymi wpływu na kształtowanie polityki państwa lub sprawowanie władzy publicznej, opierającą swoją działalność na pracy społecznej członków. Mając na uwadze powyższe stwierdzić należy, że prowadzone przez partie polityczne zbiory danych osób zrzeszonych w tych partiach nie podlegają obowiązkowi zgłoszenia do rejestracji. Po drugie, stosownie do treści przepisu art. 43 ust. 1 pkt 6 ustawy, z obowiązku rejestracji zwolnieni są administratorzy danych tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województwa, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum

lokalnego.

Zatem co do zasady zbiory danych prowadzone przez partie polityczne zwolnione są z obowiązku zgłoszenia do rejestracji, jednakże mogą one prowadzić również zbiory podlegające obowiązkowi rejestracji. Przykładami takich zbiorów są: zbiory danych kandydatów na radnych, posłów, senatorów, zawierające dane osób niebędących członkami tych partii (prowadzone na innej podstawie niż przepisy dotyczące wyborów i referendów, np. na podstawie zgody osób, których dane dotyczą), zbiory danych sympatyków partii i osób zainteresowanych działalnością partii (np. zbiory danych zarejestrowane pod numerami 092642 i 099646) oraz zbiory dziennikarzy i przedstawicieli mediów, prowadzone w celu informowania o działaniach, zamierzeniach i założeniach programowych partii.

Zauważyć należy, iż zgłoszeń zbiorów danych, w których dane przetwarzane są w związku z działalnością partii politycznych oraz na potrzeby kampanii wyborczych dokonują również podmioty niebędące partiami politycznymi. Przykładem może być zbiór danych zgłoszony przez osobę fizyczną prowadzącą działalność gospodarczą, utworzony w związku z funkcjonowaniem platformy internetowej oferującej kandydatom w wyborach samorządowych zamieszczanie wpisów zawierających informacje o sobie i swojej działalności politycznej, w postaci zdjęć, filmów, spotów wyborczych itp. (np. zbiór danych zarejestrowany pod numerem 093312). Kolejnym przykładem jest zbiór prowadzony przez spółkę z ograniczoną odpowiedzialnością, który zawiera dane sympatyków partii politycznej gromadzone w celu prowadzenia samorządowej kampanii wyborczej oraz kontaktowania się z sympatykami partii po wyborach w celu poznania ich poglądów na temat działań władz lokalnych (np. zbiór danych zarejestrowany pod numerem 070477). W opisanych zgłoszeniach zbiorów danych do rejestracji administratorzy jako podstawę prawną upoważniającą do prowadzenia zbioru wskazywali zazwyczaj zgodę zainteresowanej osoby na przetwarzanie danych jej dotyczących.

Zgłoszenia zbioru danych osobowych do rejestracji dokonuje się na urzędowym formularzu. Obecnie obowiązujący wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych stanowi załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536).

Na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych (www.giodo.gov.pl), w ramach Platformy e-GIODO, dostępny jest program komputerowy służący do prawidłowego wypełniania formularza zgłoszenia zbioru danych – „Wspomaganie

wypełniania wniosku”. Po wypełnieniu formularza wnioskodawca ma możliwość wysyłania (za pośrednictwem tego programu) zgłoszenia zbioru danych osobowych do rejestracji drogą elektroniczną. Jeśli wnioskodawca nie dysponuje bezpiecznym podpisem elektronicznym należy - po wysłaniu zgłoszenia drogą elektroniczną - wydrukować je, podpisać i dostarczyć w sposób tradycyjny. Trzeba podkreślić, że zgłoszenie zbioru do rejestracji nie oznacza przesyłania danych osobowych, które stanowią jego zawartość, ani dokumentów potwierdzających zawarte w nim oświadczenia, np. polityki bezpieczeństwa, czy instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Administrator danych zobowiązany jest również zgłaszać Generalnemu Inspektorowi każdą zmianę informacji zawartych w zgłoszeniu (art. 41 ust. 2, 3 i 4 ustawy). Zgłoszenia zmian dokonuje się na tym samym formularzu, który służy do zgłaszania zbioru do rejestracji.

Zgłoszenia zbiorów danych rejestrowane są w ogólnokrajowym, jawnym rejestrze zbiorów danych osobowych prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych. Każdy, korzystając z prawa do przeglądania rejestru, może uzyskać ogólne informacje o administratorach danych i prowadzonych przez nich zbiorach. Informacje zawarte w rejestrze udostępniane są na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych (www.giodo.gov.pl) w ramach Platformy e-GIODO.

VI. PYTANIA I ODPOWIEDZI

Czy komitet wyborczy może przysyłać komunikaty marketingowe w sposób automatyczny bez wcześniejszej zgody adresatów?

Nie. Zgodnie z art. 172 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 z późn. zm.), zakazane jest używanie automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę. W myśl art. 209 ust. 1 pkt 25 Prawa telekomunikacyjnego, kto nie wypełnia obowiązków uzyskania zgody abonenta lub użytkownika końcowego, o której mowa m.in. w art. 172, podlega karze pieniężnej. Karę tę nakłada prezes Urzędu Komunikacji Elektronicznej (UKE), w drodze decyzji, po przeprowadzeniu w sprawie stosownego postępowania. Zatem jeżeli działalność operatora telekomunikacyjnego narusza wymieniony przepis, można zwrócić się w tej sprawie również do UKE z prośbą o jej rozpoznanie.

Czy można odmówić podania informacji zawierających dane służbowe (adres poczty elektronicznej, numer telefonu) funkcjonariusza publicznego sprawującego urząd z wyboru i kandydującego w wyborach?

Nie. Dane w zakresie służbowego adresu poczty elektronicznej oraz numeru telefonu są danymi jawnymi i odmowa ich udostępnienia z powołaniem się na przepisy ustawy o ochronie danych osobowych nie znajduje podstaw. Dane służbowe są ściśle związane z pełnieniem funkcji publicznej przez takiego funkcjonariusza i mogą być wykorzystane (udostępniane) nawet bez jego zgody.

Wskazują na to przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782 z późn. zm.). Zgodnie z art. 2 ust. 1 ustawy o dostępie do informacji publicznej, na zasadach i w trybie określonym w jej przepisach, każdemu przysługuje prawo dostępu do informacji publicznej. Informacją publiczną jest każda informacja o sprawach publicznych. Prawo to podlega ograniczeniu jedynie w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, jak również ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz w przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa (art. 5 ust. 1 i 2 ustawy o dostępie do informacji publicznej).

Czy komitet wyborczy może rozsyłać imienne adresowane ulotki wyborcze i listy agitacyjne do adresatów, których dane jeden z kandydatów zebrał jako wolontariusz w trakcie wcześniejszej kampanii wyborczej prowadzonej na rzecz kandydata na Prezydenta RP?

Nie. Procedurę zbierania danych osobowych od osób popierających określoną kandydaturę na urząd Prezydenta RP, w tym zakres danych, regulowały dotychczas przepisy ustawy z dnia 27 września 1990 r. o wyborze Prezydenta Rzeczypospolitej Polskiej (Dz. U. z 2010 r. Nr 72, poz. 467 z późn. zm.). sposób zbierania podpisów osób popierających

zgłoszenie kandydata na Prezydenta RP określał art. 40g powołanej ustawy. Natomiast z przepisu art. 41 ust. 1 pkt 3 tego aktu wynika, że zgłoszenie kandydata na Prezydenta RP powinno zawierać wykaz obywateli popierających zgłoszenie, zawierający czytelne wskazanie imienia (imion) i nazwiska, adresu zamieszkania oraz numeru ewidencyjnego PESEL obywatela, który udziela poparcia, składając na wykazie własnoręczny podpis; każda strona wykazu musi zawierać nazwę komitetu zgłaszającego kandydata oraz adnotację: „Udzielam poparcia kandydatowi na Prezydenta Rzeczypospolitej Polskiej (imię/imiona i nazwisko kandydata) w wyborach przypadających w ... roku”. Stosownie zaś do art. 42 powołanej ustawy, Państwowa Komisja Wyborcza (PKW) zarejestruje kandydata na Prezydenta Rzeczypospolitej, jeżeli zgłoszenia dokonano zgodnie z przepisami tej ustawy, sporządzając protokół rejestracji kandydata i zawiadania o tym pełnomocnika wyborczego (ust. 1). PKW, sprawdzając prawidłowość zgłoszenia kandydata, bada, czy zgłoszenie kandydatury poparto podpisami co najmniej 100 000 obywateli (ust. 2 pkt 3).

Z przywołanych przepisów ustawy o wyborze Prezydenta RP wynika zatem, że dane osobowe osób popierających zgłoszenie kandydata na Prezydenta RP zbierane były w jednym, konkretnym celu – do zgłoszenia i rejestracji przez Państwową Komisję Wyborczą określonej kandydatury oraz ewentualnej weryfikacji tego zgłoszenia. Natomiast przepisy tego aktu, jak i obowiązującego od 1 sierpnia 2011 r. Kodeksu wyborczego (art. 303 § 1 pkt 3) nie przewidują kopiowania list zawierających podpisy poparcia i wykorzystywania ich w jakikolwiek inny sposób.

Czy burmistrz w trakcie kampanii wyborczej może wykorzystać do celów związanych z własną kampanią wyborczą dane osobowe mieszkańców znajdujące się w zbiorze danych osobowych urzędu gminy?

Nie. Ewidencja ludności prowadzona jest na podstawie ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2015 r. poz. 338). Żaden z przepisów tej ustawy nie daje podstaw do wykorzystywania danych osobowych mieszkańców gminy do prowadzenia przez burmistrza własnej kampanii wyborczej. W opisanym przypadku udostępnienie danych do tego celu mogłoby nastąpić tylko na podstawie zgody świadomie wyrażonej przez podmiot danych. Zgoda zaś nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści (art. 7 ust. 5 ustawy). W tym przypadku doszłoby więc do nieuprawnionego wykorzystania danych osobowych pochodzących ze zbiorów urzędowych do prowadzenia własnej kampanii wyborczej przez osobę sprawującą funkcję publiczną.

Czy wyborca ma prawo do kontroli swoich danych, które są przetwarzane przez komitet wyborczy?

Tak. Zgodnie z art. 32 ust. 1 ustawy, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, także w związku z kampanią wyborczą. Każda osoba ma prawo do żądania:

- uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna – jej miejsca zamieszkania oraz imienia i nazwiska;
- uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
- uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
- uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.

Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić wymienionych wcześniej informacji odnośnie do jej danych osobowych.

Jakie są podstawy prawne przetwarzania danych osobowych w spisach wyborców?

Podstawę przetwarzania danych w spisach wyborców stanowi art. 26 § 1. Stosownie do tej regulacji, osoby, którym przysługuje prawo wybierania, wpisuje się do spisu wyborców.

Zgodnie z art. 35 § 1 Kodeksu wyborczego, wyborcy przebywający za granicą i posiadający ważne polskie paszporty lub – w przypadku obywateli Unii Europejskiej niebędących obywatelami polskimi – posiadający ważny paszport lub inny dokument stwierdzający tożsamość, wpisywani są do spisu wyborców sporządzanego przez właściwego terytorialnie konsula. Stosownie do art. 35 § 2, wpisu dokonuje się na podstawie osobistego zgłoszenia wniesionego ustnie, pisemnie, telefonicznie, telegraficznie, telefaksem lub w formie elektronicznej. Zgłoszenie powinno zawierać imię (imiona), imię ojca, datę

urodzenia, numer ewidencyjny PESEL, oznaczenie miejsca pobytu wyborcy za granicą, numer ważnego polskiego paszportu, a także miejsca i datę jego wydania, a w przypadku obywateli polskich czasowo przebywających za granicą, również miejsce wpisania wyborcy do rejestru wyborców. W przypadku obywateli Unii Europejskiej niebędących obywatelami polskimi, zgłoszenie powinno zawierać numer innego ważnego dokumentu stwierdzającego tożsamość, a także miejsce i datę jego wydania. Zgłoszenia można dokonać najpóźniej w 3 dniu przed dniem wyborów. Mając na uwadze konieczność zapewnienia możliwości weryfikacji danych zawartych w spisie wyborców przebywających za granicą, bezpieczeństwa wprowadzania i przetwarzania tych danych, ich przekazywania i odbioru oraz zasadę, zgodnie z którą można być wpisanym tylko do jednego spisu wyborców, minister właściwy do spraw zagranicznych został upoważniony, po zasięgnięciu opinii Państwowej Komisji Wyborczej, do określenia, w drodze rozporządzenia, sposobu sporządzania i aktualizacji spisu wyborców, a także sposobu powiadamiania urzędów gmin o objętych spisem wyborców osobach stale zamieszkałych w kraju i sposobu wydawania i ewidencjonowania zaświadczeń o prawie do głosowania.

Czy wyborca ma prawo odmówić okazania dokumentu tożsamości komisji wyborczej?

Nie. Zgodnie z art. 52 § 1 ustawy Kodeks wyborczy, przed przystąpieniem do głosowania wyborca okazuje obwodowej komisji wyborczej dokument umożliwiający stwierdzenie jego tożsamości. Zgodnie natomiast z § 2 tego artykułu, po wykonaniu czynności, o której mowa w § 1, wyborca otrzymuje od komisji kartę do głosowania właściwą dla przeprowadzanych wyborów, opatrzoną jej pieczęcią. Wyborca potwierdza otrzymanie karty do głosowania własnym podpisem w przeznaczony na to rubryce spisu wyborców. Odmienności związane z głosowaniem poza granicami kraju określa 52 § 3.

Czy osoba, która na wykorzystywanym przez obwodową komisję wyborczą spisie wyborców składa podpis, potwierdzając odbiór kart do głosowania, ma prawo widzieć dane osobowe pozostałych osób ujętych w spisie?

Nie, dane osobowe zawarte w spisie wyborców nie powinny być widoczne dla osób, które biorąc udział w wyborach, swoim podpisem potwierdzają odbiór kart do głosowania. Kwestie związane ze sporządzaniem spisu wyborców oraz jego udostępnianiem regulują przepisy Rozdziału 5 Kodeksu wyborczego oraz przepisy rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 grudnia 2014 r. w sprawie spisu wyborców. Szczegółowo określają, na potrzeby poszczególnych wyborów, sposób sporządzania spisu wyborców i zakres

zawartych w nim danych.

Spis wyborców prowadzony jest zgodnie z art. 26 § 6 ustawy Kodeks wyborczy. Spis wyborców składa się z części A - w wyborach do Sejmu i do Senatu, w wyborach Prezydenta Rzeczypospolitej oraz w wyborach do rad powiatów i sejmików województw; z części A i części B w wyborach do Parlamentu Europejskiego w Rzeczypospolitej Polskiej. Artykuł 26 § 7 stanowi, iż część A spisu wyborców obejmuje obywateli polskich. W tej części spisu wyborców wymienia się nazwisko i imię (imiona), imię ojca, datę urodzenia, numer ewidencyjny PESEL i adres zamieszkania wyborcy. Z kolei, zgodnie z art. 26 § 8, część B spisu wyborców obejmuje obywateli Unii Europejskiej niebędących obywatelami polskimi, uprawnionych do korzystania z praw wyborczych w wyborach, które zostały zarządzane w Rzeczypospolitej Polskiej. W tej części spisu wyborców wymienia się nazwisko i imię (imiona), imię ojca, datę urodzenia, obywatelstwo państwa członkowskiego Unii Europejskiej, numer paszportu lub innego dokumentu stwierdzającego tożsamość oraz adres zamieszkania wyborcy.

Zgodnie z art. 36 § 1 Kodeksu wyborczego, między 21 a 8 dniem przed dniem wyborów każdy wyborca może sprawdzić w urzędzie gminy, w której spis wyborców został sporządzony, czy został w spisie uwzględniony. Spis wyborców jest udostępniany do wglądu w urzędzie gminy (art. 36 § 2), a wójt powiadamia wyborców, w sposób zwyczajowo przyjęty, o sporządzeniu spisu wyborców oraz o miejscu i czasie jego udostępniania (art. 36 §3). Powołane przepisy stosuje się zaś odpowiednio do innych niż gmina organów, które sporządziły spis wyborców (art. 36 § 4).

Sposób sporządzenia i udostępniania spisu wyborców szczegółowo reguluje - wydane na podstawie art. 33 Kodeksu wyborczego – rozporządzenie Ministra Spraw Wewnętrznych z dnia 29 grudnia 2014 r. w sprawie spisu wyborców. Zgodnie z jego przepisami, udostępnienie spisu wyborców następuje na pisemny wniosek wyborcy (§ 15 ust. 1). Wzór takiego wniosku zawarty został w załączniku nr 6 do rozporządzenia. Osoba składająca wniosek musi podać takie swoje dane, jak: imię (imiona), nazwisko i adres zamieszkania i może prosić o potwierdzenie, że figuruje w spisie wyborców. Jak bowiem stanowi § 16 powołanego rozporządzenia, udostępnianie spisu wyborców do wglądu następuje przez udzielenie informacji, że osoba wskazana we wniosku jest ujęta w spisie wyborców lub nie figuruje w spisie, w tym również z powodu skreślenia ze spisu, albo że dane wpisane we wniosku różnią się od danych osoby wpisanej do spisu wyborców. Oznacza to, że wgląd do spisu wyborców nie jest tożsamy z dostępem do danych wszystkich osób, które są w nim ujęte. Prawo wglądu do spisu wyborców przysługuje jedynie wyborcy w celu sprawdzenia,

czy został on uwzględniony w spisie, obejmuje zatem swym zakresem tylko i wyłącznie kontrolę danych osoby fizycznej, której dane dotyczą. Na żądanie wnioskodawcy udzielona informacja jest potwierdzana na piśmie (§ 16 rozporządzenia).

Podkreślić należy, że przepisy regulujące kwestię przeprowadzania wyborów nie przewidują w swoich regulacjach możliwości dostępu do danych osobowych osób innych niż osoba, której dane dotyczą. Powyższe odnosi się zarówno do sytuacji weryfikowania danych zawartych w spisie wyborców przed rozpoczęciem wyborów, jak i w momencie potwierdzania otrzymania karty do głosowania.

Stanowisko to potwierdza również doktryna. Jak wskazuje dr Andrzej Kisielewicz, Kodeks wyborczy nie przewiduje takiej jawności spisu wyborców, o jakiej mowa w odniesieniu do rejestru wyborców (art. 18 § 12 Kodeksu wyborczego). Dopuszcza jedynie możliwość sprawdzenia przez wyborcę, czy ten został uwzględniony w spisie. Ogranicza więc znacząco dostęp wyborców do spisu wyborców. Przepis art. 36 § 2 interpretowany z uwzględnieniem treści § 1 tego artykułu nakazuje bowiem przyjąć, że prawo wglądu do spisu wyborców przysługuje jedynie wyborcy w celu sprawdzenia, czy został on uwzględniony w spisie, obejmuje zatem informacje na jego temat. Można na tej podstawie powiedzieć, że ustawodawca, przyznając pierwszeństwo ochronie danych osobowych, nie zapewnił szerszej, społecznej kontroli nad sporządzaniem i prowadzeniem spisów wyborców, istotnej z punktu widzenia przestrzegania kardynalnych zasad prawa wyborczego: powszechności i równych praw wyborczych. Dr Andrzej Kisielewicz przesądza również, że (...) w sprawach dotyczących udostępniania spisu wyborców do wglądu wyborców mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Wynika to z art. 3 ust. 1 tej ustawy, stanowiącego o jej stosowaniu do organów państwowych i samorządowych, a także z art. 6 ust. 1 i 2 w zw. z art. 1 ust. 1 ustawy, gwarantujących każdemu prawo do ochrony jego danych osobowych, którymi w rozumieniu ustawy są wszelkie informacje umożliwiające zidentyfikowanie tożsamości danej osoby; takie zaś informacje zawierają dane o wyborcach umieszczonych w spisie wyborców.” (dr Andrzej Kisielewicz, Komentarz, Kodeks wyborczy, LEX, 2014).

Zatem, wszystkie podmioty zaangażowane w organizację i przeprowadzenie wyborów muszą przestrzegać nie tylko przepisów szczególnych, bezpośrednio regulujących ich przebieg, ale również przepisów ustawy o ochronie danych osobowych.

Zobowiązują one każdego, kto przetwarza dane osobowe do należytej o nie dbałości, a przepisy jej rozdziału 5 określają ogólne zasady ich zabezpieczenia. Zgodnie zaś z jej art. 36 ust. 1, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne

zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wybór odpowiednich środków gwarantujących przetwarzanym danym optymalny stopień zabezpieczenia pozostawia jednak do uznania konkretnemu administratorowi danych osobowych. Ważne jest, aby administrator danych dysponował takimi instrumentami organizacyjnymi i technicznymi, za pomocą których będzie w stanie wyeliminować zagrożenia utraty, zmiany czy zniszczenia danych osobowych.

Wypełnienie obowiązków wynikających z rozdziału 6 ustawy o ochronie danych osobowych, m.in. nieudostępniania danych osobowych osobom do tego nieupoważnionym, może być zrealizowane – tak jak zostało to przeprowadzone w Łodzi – poprzez użycie specjalnego szablonu nakładanego na spisy wyborców. Jest to przesuwana, kartonowa nakładka z wyciętym otworem. Dzięki niej wyborcy, którzy odbierając karty do głosowania składają podpis na spisie wyborców, mogą sprawdzić tylko własne dane, reszta spisu jest bowiem zasłonięta.

Gdzie szukać pomocy

Infolinia, tel. 022, 860 70 70

Poniedziałek - piątek, godz. 8.00-16.00

Konsultacje z prawnikami

Poniedziałek - piątek, godz. 8.00-16.00

Biuro Generalnego Inspektora Ochrony Danych Osobowych

ul. Stawki 2, budynek INTRACO

00-193 Warszawa

kancelaria@giodo.gov.pl

www.giodo.gov.pl

Bezpłatne kursy e-learningowe

Każdy, kto chce pogłębić swoją wiedzę na temat ochrony danych osobowych może skorzystać z internetowego serwisu edukacyjnego, tzw. platformy eduGIODO. Dzięki temu portalowi możliwe jest zapoznanie się z podstawowymi zagadnieniami dotyczącymi ochrony danych osobowych i ukończenie trzech specjalistycznych kursów e-learningowych wzbogaconych o elementy multimedialne oraz testy sprawdzające wiedzę.

www.edugiodo.gov.pl