Drohiczyn 2019-09-16

Instrukcja postępowania

z danymi osobowymi w czasie wyborów do Sejmu i Senatu 2019r.

§ 1.

Dane osobowe

1. Dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
2. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (przykładowo numer PESEL), dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
3. Z zasady zakazane jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, jednakże w procesie wyborczym dopuszczalne jest przetwarzanie danych osobowych mogących ujawniać poglądy polityczne (przykładowo dane o przynależności do partii politycznych kandydatów, poparcie przez wyborcę na liście poparcia konkretnego kandydata, wpłata na konkretny komitet wyborczy), danych o stanie zdrowia (w przypadku zgłoszenia zamiaru głosowania korespondencyjnego lub przez pełnomocnika) lub danych na temat wyroków skazujących (przetwarzanie danych dopuszczalne wyłącznie pod nadzorem władz publicznych).

§ 2.

Przetwarzanie danych osobowych

1. Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
2. Organy wyborcze, w tym gminne i obwodowe komisje wyborcze, obowiązane na podstawie przepisów prawa do przeprowadzenia wyborów, są uprawnione do przetwarzania danych osobowych w zakresie niezbędnym do zrealizowania tego zadania.

§ 3.

Zasady przetwarzania danych osobowych

W procesie wyborczym dane osobowe winny być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą;
b) zbierane wyłącznie w celu przeprowadzenia wyborów;

c) gromadzone w zakresie niezbędnym dla przeprowadzenia wyborów, wynikającym z obowiązujących przepisów;
d) prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celu przetwarzania sprostowane albo usunięte;
e) przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne do realizacji celu przetwarzania;
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkowa utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

§ 4.

Administrator danych osobowych

1. Administratorami danych osobowych są organy wyborcze, działające w celu przeprowadzenia wyborów w wykonaniu zadań określonych przepisami prawa.
2. Do podstawowych obowiązków administratora danych osobowych w procesie wyborczym należą:
   a) zabezpieczenie danych osobowych przed nieuprawnionym dostępem;
   b) zabezpieczenie danych osobowych przed zniszczeniem lub utratą;
   c) prowadzenie rejestru czynności przetwarzania;
   d) wyznaczenie inspektora ochrony danych;
   e) zgłaszanie Prezesowi Urzędu Ochrony Danych Osobowych naruszeń ochrony danych.

§ 5.

Środki służące zabezpieczeniu przetwarzanych danych

1. Dobór środków służących zabezpieczeniu przetwarzanych danych musi uwzględniać czynniki o charakterze technicznym i organizacyjnym, w szczególności sprzęt, system informatyczny, ilość pomieszczeń, jakimi dysponuje dana komisja wyborcza oraz prawdopodobieństwo i wagę ewentualnego zagrożenia dla danych osobowych.
2. Do środków służących zabezpieczeniu danych zalicza się w szczególności:
   a) pseudonimizację i szyfrowanie danych osobowych;
   b) zdolność zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolność szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
   e) prowadzenie rejestru czynności przetwarzania.
3. Korzystanie z systemów teleinformatycznych, rejestrów publicznych i wymiana informacji w postaci elektronicznej przez organy wyborcze odbywa się z zachowaniem wymogów określonych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247 tj.).

§ 6.

Rejestr czynności przetwarzania

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych w formie pisemnej, w tym elektronicznej.
2. W rejestrze zamieszcza się następujące informacje:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz współadministratorów, a także gdy ma to zastosowanie przedstawiciela administratora oraz inspektora danych;
   b) cele przetwarzania;
   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
   e) gdy ma to zastosowanie, o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa art. 49 ust. 1 akapit drugi Rozporządzenia 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) - RODO, dokumentacja odpowiednich zabezpieczeń;
   f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

§ 7.

Inspektor ochrony danych

1. Administrator wyznacza inspektora ochrony danych.
2. O wyznaczeniu inspektora ochrony danych zawiadamia się prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia jego wyznaczenia w trybie uregulowanym w art. 10 Ustawy z 10.05.2018 r. o ochronie danych osobowych - Dz. U. z 2018 r. poz. 1000 (zgłoszenie wyłącznie w postaci elektronicznej).
3. Administrator udostępnia dane inspektora, w tym jego imię i nazwisko, numer telefonu oraz adres poczty elektronicznej w sposób ogólnie dostępny.
4. Do zadań inspektora ochrony danych należy:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia 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) - RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania przepisów Rozporządzenia 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) - RODO, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w

dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
d) współpraca z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, konsultacjami z organem nadzorczym oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

§ 8.

Naruszenie ochrony danych osobowych

1. Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych stanowi naruszenie ochrony danych osobowych.
2. W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Zgłoszenie zawiera co najmniej:
   a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   d) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki.
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

§ 9.

Okres przechowywania danych

1. Dokumenty z wyborów są przechowywane przez okres co najmniej 5 lat.
2. Organy wyborcze przechowują dokumenty z wyborów do dnia ich brakowania bądź przekazania do archiwum na podstawie odrębnych przepisów.

BURMISTRZ

mgr inż. Wojciech Borzym