Kategoria: Aktualności
Opublikowano: piątek, 02, wrzesień 2011 00:00
Rafał Rudka
Odsłony: 2188

Zabezpieczanie danych osobowych przetwarzanych na potrzeby kampanii wyborczej

Ustawa w swoim 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych, wyznacza także administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, chyba że sam wykonuje te czynności.

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 do osób, które przetwarzają dane 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.

Kategoria: Aktualności
Opublikowano: piątek, 02, wrzesień 2011 00:00
Rafał Rudka
Odsłony: 2188

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 informacyjnymi, 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 zależny jest od zastosowanych nośników informacji, rodzaju 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 tych 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 przekazane 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.

Kategoria: Aktualności
Opublikowano: piątek, 02, wrzesień 2011 00:00
Rafał Rudka
Odsłony: 2188

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.

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 ust. 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 się dopiero po zarejestrowaniu zbioru.

Zgłoszenie zbioru danych do rejestracji jest zasadą, od której wyjątki wymienione zostały w art. 43 ust. 1 pkt 1–11 ustawy. 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.

Kategoria: Aktualności
Opublikowano: piątek, 02, wrzesień 2011 00:00
Rafał Rudka
Odsłony: 2188

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

Pierwszą określa 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 nie będących 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 nie będące 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.

Źródło: "Poradnik: Ochrona danych osobowych w trakcie prowadzenia kampanii wyborczej", P. Zieliński, GIODO