**Polityka bezpieczeństwa danych osobowych w organizacji pozarządowej**

**Podstawowe informacje na temat polityki bezpieczeństwa danych osobowych stosowanej przez organizację pozarządową.**

**UWAGA: Od 25 maja 2018 r. zaczynamy stosować przepisy o ochronie danych osobowych zawarte w unijnym rozporządzeniu, zwanym w skrócie RODO.**

Tym samym opisane poniżej zasady ochrony danych osobowych wynikające z polskiej ustawy o ochronie danych osobowych (z 29 sierpnia 2997 r.) przestana obowiązywać.

Nowe przepisy omawiamy m.in. w informacjach:

* [Od maja nowe zasady ochrony danych osobowych. Pierwszeństwo przepisów UE](http://www.poradnik.ngo.pl/wiadomosc/2136523.html)
* [Projekt nowej ustawy o ochronie danych osobowych. Co ważne dla organizacji pozarządowych?](http://www.poradnik.ngo.pl/wiadomosc/2120444.html)

Organizacje pozarządowe – niezależnie od swojej wielkości, zakresu działań i zasięgu terytorialnego – realizując zadania statutowe, przetwarzają dane osobowe. Są to np. dane ich członków, darczyńców, wolontariuszy, zewnętrznych odbiorców działań (tzw. beneficjentów).

Wszystkie te dane wymagają co najmniej posiadania i stosowania **polityki bezpieczeństwa danych osobowych** – nie ma tu wyjątków. Mowa jest o tym w art. 3 ust. 2 pkt 2 ustawy o ochronie danych osobowych:

Ustawę stosuje się również do: osób fizycznych i osób prawnych (od red.: czyli np. stowarzyszeń, fundacji) oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych, które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Niektóre dane osobowe wymagają też rejestracji u Generalnego Inspektora Ochrony Danych Osobowych (GIODO), np. dane dotyczące wolontariuszy, darczyńców. W dużym skrócie można powiedzieć, że rejestruje się dane osobowe osób z zewnątrz, spoza organizacji, a nie rejestruje danych osób związanych z organizacją, „z wewnątrz”, np. danych członków stowarzyszenia, pracowników i współpracowników organizacji.

Pamiętajmy też, że prowadzenie bazy danych w komputerze, np. w Excelu, wymaga posiadania  dodatkowego dokumentu, czyli  instrukcji bezpiecznego zarządzania systemem informatycznym.

Czym jest zatem obowiązkowa polityka bezpieczeństwa? To zestaw reguł, praw i praktycznych zasad regulujących sposób przetwarzania danych wewnątrz organizacji (zarządzanie, ochrona, dystrybucja).

**Kiedy organizacja musi mieć politykę bezpieczeństwa**

Ustawa o ochronie danych osobowych nakłada na wszystkich administratorów danych obowiązek stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz zabezpieczenia ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jednym z podstawowych wymogów w tym zakresie jest opracowanie i wdrożenie **polityki bezpieczeństwa**, o której mowa w przepisach wykonawczych do ustawy.

W praktyce odpowiedzialność za posiadanie i stosowanie polityki ponosi zarząd organizacji, który powinien zadbać o opracowanie polityki bezpieczeństwa i podjąć uchwałę w sprawie jej przyjęcia.

PRZYKŁAD:

Organizacja zajmuje się edukacją – organizuje zajęcia dla dzieci w wieku szkolnym.  W związku z tym prowadzi bazę danych w Excelu, w której zbiera ich dane oraz telefony kontaktowe do rodziców, opiekunów (formalnie są to przedstawiciele ustawowi małoletnich dzieci).

Prawnie oznacza to, że organizacja przetwarza dane osobowe i musi mieć uchwaloną, podpisaną oraz wdrożoną politykę bezpieczeństwa (włącznie z dopuszczeniem do przetwarzania danych osobowych osób, które muszą mieć pisemne upoważnienie do przetwarzania danych oraz prowadzeniem ewidencji osób upoważnionych do przetwarzania danych osobowych).

UWAGA!

Ponieważ organizacja prowadzi bazę danych w Excelu,  musi też mieć dodatkowy dokument, czyli instrukcję bezpiecznego zarządzania systemem informatycznym.

W tym przypadku organizacja musi też zgłosić zbiór danych do rejestracji GIODO (gromadzi dane osobowe osób „z zewnątrz”, spoza organizacji). Jeśli w zbiorze tym przetwarzane są tylko dane osobowe (np. imię i nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania / pobytu, numer telefonu), organizacja będzie mogła przetwarzać dane od momentu dokonania zgłoszenia zbioru danych do rejestracji GIODO. Jeśli natomiast w zbiorze tym organizacja z uzasadnionych powodów zamierzałaby jeszcze przetwarzać np. dane o stanie zdrowia (są to tzw. dane wrażliwe, sensytywne) to wówczas przetwarzanie danych w ramach tego zbioru będzie możliwe dopiero po wydaniu przez GIODO zaświadczenia o zarejestrowaniu zbioru danych. Procedura rejestracji zbioru danych obejmującego dane wrażliwe trwa od 3 miesięcy do roku lub dłużej.

PRZYKŁAD:

Organizacja zbiera podstawowe dane o swoich wolontariuszach i darczyńcach, aby móc się z nimi kontaktować.

Oba zbiory danych dotyczą osób spoza organizacji, a zatem jest ona zobligowana do:

* zapewnienia ochrony danych poprzez posiadanie opracowanej i wdrożonej polityki bezpieczeństwa (włącznie z dopuszczeniem do przetwarzania danych osobowych tylko osób posiadających pisemne upoważnienie do ich przetwarzania oraz prowadzeniem ewidencji osób upoważnionych do przetwarzania danych osobowych),
* oraz zgłoszenia tych zbiorów (każdego oddzielnie) do rejestracji w GIODO.

W zbiorach tych przetwarzane są tylko „zwykłe” dane osobowe (np. imię, nazwisko, adres zamieszkania, numer telefonu, adres poczty elektronicznej) – zatem organizacja może przetwarzać te dane już od momentu dokonania zgłoszenia zbioru danych do rejestracji w GIODO.

PRZYKŁAD:

Organizacja zbiera dane o stanie zdrowia swoich podopiecznych w związku z prowadzonym gabinetem rehabilitacyjnym.

Są to dane wrażliwe. Należą do nich dane ujawniające bezpośrednio lub w kontekście: pochodzenie rasowe, pochodzenie etniczne, poglądy polityczne, przekonania religijne, przekonania filozoficzne, przynależność wyznaniową, przynależność partyjną, przynależność związkową, stan zdrowia, kod genetyczny, nałogi, życie seksualne. W praktyce organizacje najczęściej stykają się z danymi dotyczącymi stanu zdrowia, stopnia niepełnosprawności. Jeśli organizacja podejmuje działania na rzecz osób niepełnosprawnych, chorych, np. prowadzi gabinet (realizuje jakiś projekt):

* i projekt ten jest skierowany tylko do członków (np. stowarzyszenie zrzesza osoby niepełnosprawne) – wówczas organizacja zobligowana jest do zapewnienia ochrony danym wrażliwym poprzez posiadanie opracowanej i wdrożonej polityki bezpieczeństwa (włącznie z dopuszczeniem do przetwarzania danych osobowych tylko osób mających pisemne upoważnienie do ich przetwarzania oraz prowadzeniem ewidencji tych osób); nie musi natomiast zgłaszać zbioru danych do GIODO (gdyż projekt jest skierowany do członków stowarzyszenia, a dane członków nie podlegają rejestracji);
* i projekt ten jest skierowany także do osób z zewnątrz – organizacja jest wówczas zobligowana do zapewnienia ochrony danym wrażliwym poprzez posiadanie opracowanej i wdrożonej polityki bezpieczeństwa (włącznie z dopuszczeniem do przetwarzania danych jedynie osób mających pisemne upoważnienie do ich przetwarzania oraz prowadzeniem ewidencji tych osób) oraz do zgłoszenia tego zbioru danych do GIODO (ponieważ są to dane osób „z zewnątrz” organizacji). Przetwarzanie danych w ramach tego zbioru będzie możliwe dopiero po wydaniu przez GIODO zaświadczenia o rejestracji zbioru danych. Procedura rejestracji zbioru danych obejmującego dane wrażliwe trwa od 3 miesięcy do roku lub nawet dłużej.

PRZYKŁAD:

Organizacja rekrutuje nowego pracownika do rozpoczynającego się projektu.

Przetwarzanie danych kandydatów do pracy również wymaga zapewnienia im ochrony poprzez opracowanie i wdrożenie polityki bezpieczeństwa (włącznie z dopuszczeniem do przetwarzania danych jedynie osób mających pisemne upoważnienie do ich przetwarzania oraz prowadzeniem ewidencji tych osób). Nie wymaga to natomiast zgłoszenia zbioru danych do GIODO.

PRZYKŁAD:

Organizacja zatrudnia pracowników, zleca też prace na umowy o dzieło.

Przetwarzanie danych pracowników (zatrudnionych na umowę o pracę) oraz współpracowników (umowy zlecenia, umowy o dzieło) wymaga zapewnienia im ochrony poprzez opracowanie i wdrożenie polityki bezpieczeństwa (włącznie  
z dopuszczeniem do przetwarzania danych tylko osób posiadających pisemne upoważnienie do ich przetwarzania oraz prowadzeniem ewidencji tych osób). Nie wymaga to natomiast zgłoszenia zbioru danych do GIODO.

UWAGA!

Prowadzenie bazy danych w Excelu, programie Płatnik, innych programach posiadających moduły kadrowo-płacowe, wymaga posiadania przez organizację dodatkowego dokumentu, czyli instrukcji bezpiecznego zarządzania systemem informatycznym.

**Dodatkowo, jeśli pieniądze z UE**

Organizacje realizujące projekty współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego (np. PO KL) zobowiązane są dodatkowo (poza obowiązkami wynikającymi z ustawy o ochronie danych osobowych) do zapewnienia ochrony przetwarzanym danym osobowym beneficjentów zgodnie z zapisami umowy o dofinansowanie realizacji projektu zawieranej pomiędzy organizacją a instytucją pośredniczącą. Obowiązek ten dotyczy danych osobowych beneficjentów przetwarzanych w formie tradycyjnej (papierowej) oraz w ramach systemu PEFS. Wywiązywanie się organizacji z tego obowiązku weryfikowane jest podczas kontroli prowadzonych przez upoważnionych pracowników instytucji pośredniczących (urzędów marszałkowskich) / instytucji pośredniczących II stopnia (wojewódzkich urzędów pracy) w trakcie realizacji projektu albo po jej zakończeniu. Organizacja realizująca taki projekt (z okresu programowania 2007-2013) zobowiązana jest przechowywać dokumentację dotyczącą jego realizacji do dnia 31 grudnia 2020 r.

**Co zyskujemy dzięki polityce bezpieczeństwa**

UWAGA!

Ustawodawca nie przewiduje w ustawie o ochronie danych osobowych kary za brak polityki bezpieczeństwa, ale jeśli organizacja nie zgłosi do rejestracji zbioru danych darczyńców czy wolontariuszy, a mimo to przetwarza je, poniesie karę (grzywna, kara ograniczenia wolności albo pozbawienia wolności do roku). Z kolei bez opracowanej i wdrożonej polityki bezpieczeństwa nie jest możliwe dokonanie zgłoszenia zbioru danych osobowych do GIODO (część E, pkt 16, ppkt „d” zgłoszenia, o którym mowa w załączniku do rozporządzenia MSWiA z dnia 11 grudnia 2008 r., Dz. U. Nr 229, poz. 1536).

Stosowanie w codziennym życiu organizacji zasad wynikających z polityki bezpieczeństwa pozwala na:

* legalne przetwarzanie danych osobowych i danych wrażliwych.. Bez posiadania opracowanej  i wdrożonej polityki bezpieczeństwa w zakresie ochrony danych osobowych (oraz instrukcji zarządzania systemem informatycznym, jeśli przetwarzamy dane w systemach informatycznych, komputerze) nie jest możliwe zgłoszenie zbioru danych do rejestracji w GIODO;
* zapewnienie ochrony przetwarzanym danym osobowym i nierzadko danym wrażliwym, np. dotyczącym stanu zdrowia, stopnia niepełnosprawności;
* w przypadku kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych prowadzonej przez GIODO lub np. instytucje nadzorujące realizację projektów współfinansowanych ze środków Unii Europejskiej (np. z PO KL) – okazanie dokumentów dotyczących stosowanych procedur w zakresie przetwarzania i ochrony danych osobowych;
* uniknięcie kar (grzywny, ograniczenia wolności albo pozbawienia wolności do roku albo od roku do lat 3) za niedopełnienie obowiązków wynikających z ustawy albo z zapisów umowy o dofinansowanie realizacji projektu PO KL.

**Wzór polityki bezpieczeństwa danych osobowych**

Jednym z obowiązków administratora danych (np. stowarzyszenia, fundacji) jest przygotowanie i wdrożenie tzw. polityki bezpieczeństwa. Polityka bezpieczeństwa to zestaw reguł, praw i praktycznych zasad regulujących sposób przetwarzania danych wewnątrz organizacji (zarządzanie, ochrona i dystrybucja). Celem polityki jest wskazanie działań, które muszą (lub mogą) się zdarzyć, aby organizacja - jako administrator danych, właściwie wykonała swoje obowiązki w zakresie zabezpieczenia danych, które posiada.

UWAGA!

Polityka bezpieczeństwa powinna być stworzona zawsze, jeżeli przetwarzamy jakieś dane, nie ma więc znaczenia, czy podlegają one rejestracji w GIODO.

Polityka bezpieczeństwa zawiera w szczególności:

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

**Przykładowy wzór polityki bezpieczeństwa danych osobowych -**[**kliknij, aby pobrać**](http://poradnik.ngo.pl/files/poradnik.ngo.pl/public/WZOR_polityki_bezpieczenstwa_dane_osobowe_organizacje_pozarzadowe.rtf).

Załączony wzór polityki bezpieczeństwa jest wariantem rozszerzonym, który każda organizacja może modyfikować dostosowując go do swoich potrzeb. W swojej najbardziej podstawowej i obowiązkowej wersji polityka bezpieczeństwa ogranicza się do wyżej wymienionych pięciu punktów oraz wg wskazówek poniżej:

* rozdział 1 jest obowiązkowy,
* rozdziały 2, 3, i 4 są fakultatywne – w przypisach przy ich tytułach we wzorze zawarte są informacje, że jeśli taka sytuacja nie występuje w organizacji to rozdział można pominąć (nie zawrzeć w swoim wzorze polityki),
* rozdział 5 jest fakultatywny, dotyczy tylko organizacji realizujących projekty PO KL – informacja o tym znajduje się w przypisie we wzorze polityki (pod tym adresem: <http://pokl.wup.lodz.pl/index.php/component/content/article/1-latest-news/1813-80710> znajduje się wzór opracowania na ten temat wraz z informacją, że po dostosowaniu do warunków organizacji można go umieścić w treści polityki bezpieczeństwa lub przyjąć do stosowania odrębną uchwałą zarządu)
* rozdziały 6, 7, 8, 9 i 10 oraz część II i III przydadzą się w każdej organizacji,
* załączniki od 1 do 11 znajdą zastosowanie w każdej organizacji; załączniki 12 „A” i 12 „B” natomiast dotyczą rozdziału 3 (który jest fakultatywny).

**Pamiętać należy, że polityka bezpieczeństwa:**

* powinna być aktualizowana – ponieważ organizacje rozwijają się, poszerzają zakres swoich działań i ich regulacje wewnętrzne powinny za tym nadążać,
* jest to dokument wewnętrzny, wprowadzany do stosowania w organizacji uchwałą zarządu – po odpowiednim dostosowaniu załączonego wzoru do potrzeb danej organizacji należy przygotować stronę tytułową, która może dodatkowo zawierać informacje o dacie opracowania dokumentu oraz początku jego obowiązywania.

**Odpowiedzialność zarządu**

Przyjęcie polityki powinno wynikać z uchwały zarządu organizacji. W załączonym wzorze polityki bezpieczeństwa jest o tym mowa w dwóch miejscach:

* definicje w pkt 6 (w którym jest mowa o Administratorze Bezpieczeństwa Informacji) – trzeba tam wpisać datę podjęcia uchwały zarządu wprowadzającej politykę bezpieczeństwa oraz numer tej uchwały,
* rozdział 9 Postanowienia końcowe pkt 8 – polityka bezpieczeństwa wchodzi w życie z dniem podjęcia uchwały zarządu organizacji lub w terminie określonym w treści tej uchwały (czyli zaczyna obowiązywać od momentu podjęcia uchwały albo organizacja daje sobie trochę czasu na zapoznanie się z nią wszystkich zainteresowanych osób i w treści uchwały określa początek terminu obowiązywania polityki).

Oprócz polityki bezpieczeństwa organizacja powinna także stworzyć instrukcję zarządzania systemem informatycznym, jeśli przetwarza dane osobowe w ten sposób. Instrukcja zawiera na przykład takie informacje: procedury tworzenia kopii zapasowych zbiorów danych, sposób i miejsce przechowywania tych kopii, a także wszelkich innych elektronicznych nośników informacji, procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji.

*Źródło: http://poradnik.ngo.pl/polityka-bezpieczenstwa-danych-osobowych*