Katarzyna Sadło

Ochrona danych osobowych w organizacjach pozarządowych

Ochrona danych osobowych w organizacjach pozarządowych

Redakcja i korekta:
Anna Amsterdamska

Opracowanie graficzne:
DD Studio Dariusz Piekut

Wydawca:
Fundacja Rozwoju Społeczeństwa Obywatelskiego
ul. Kłopotowskiego 6, lok. 59/60, 03-717 Warszawa
tel./faks 22 616 33 16
www.frso.pl, e-mail: frso@frso.pl

ISBN 978-83-61411-22-2

Fundator wydania:
Polsko-Amerykańska Fundacja Wolności

Spis treści

Wprowadzenie

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

(Konstytucja RP)

Przepisy ustawy o ochronie danych osobowych realizują zapisane w Konstytucji prawo każdego z nas do ochrony swojej prywatności i wszelkich danych nas dotyczących. Ustawa reguluje zasady przetwarzania danych osobowych oraz obowiązki instytucji – publicznych, prywatnych i pozarządowych – gromadzących nasze dane osobowe i wykorzystujących je w swojej działalności urzędowej, komercyjnej lub statutowej.

Organizacje pozarządowe, wbrew pokutującemu wśród nich przekonaniu, nie są podmiotowo zwolnione z obowiązków wynikających z ustawy o ochronie danych osobowych. Wiele z nich nie zna ustawy, nie wie, jakie obowiązki z niej wynikają i nie uświadamia sobie, że najprostsze czynności w bieżącej działalności – jak choćby tworzenie listy uczestników szkolenia – są przetwarzaniem danych w rozumieniu ustawy. W bazie zbiorów danych osobowych zgłoszonych do rejestracji, którą prowadzi Generalny Inspektor Ochrony Danych Osobowych, w lutym 2013 r. było tylko niecałe dwa tysiące zbiorów danych prowadzonych przez organizacje pozarządowe. Jeszcze mniej organizacji figuruje w charakterze administratorów zbiorów danych (jedna organizacja może zarejestrować kilka zbiorów), co stanowi niewielki odsetek spośród kilkudziesięciu tysięcy organizacji pozarządowych działających w Polsce. Oznacza to, niestety, że większość organizacji nie dopełniła ciążącego na nich obowiązku zarejestrowania zbiorów danych osobowych. Z dużym prawdopodobieństwem można chyba założyć, że nie są one świadome również pozostałych obowiązków wynikających z ustawy.

Publikacja ta ma przybliżyć organizacjom zagadnienie ochrony danych osobowych. Zdaję sobie sprawę, że ustawa nie jest łatwa, że przez lata „obrosła" w interpretacje i orzecznictwo, które czasem trudno ogarnąć. Zachęcam jednak do zapoznania się z tematem, w czym pomocna będzie platforma edukacyjna GIODO (www.edugiodo.gov.pl), a także do dopełnienia obowiązków wynikających z ustawy.

1

Definicje i interpretacje

Podstawa prawna

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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

Opracowanie to jest tylko wprowadzeniem do tematu ochrony danych osobowych, pomija więc regulacje międzynarodowe i inne aspekty prawa związanego z ochroną danych osobowych, które nie mają praktycznego znaczenia dla organizacji chcących tylko spełnić wymogi nałożone na nie przez prawo. Z obszernymi omówieniami przepisów polskich i międzynarodowych, a także z orzecznictwem, można zapoznać się na internetowej stronie Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Dane osobowe

Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się ***wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby*** *fizycznej. 2. Osobą możliwą do zidentyfikowania jest osoba,* ***której tożsamość można określić bezpośrednio lub pośrednio****, w szczególności* ***przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy*** *fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. 3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.*

Jak widać z powyższej ustawowej definicji, dane osobowe to nie tylko imię i nazwisko, ale także wszelkie inne informacje dotyczące konkretnej osoby fizycznej, możliwej do zidentyfikowania – bezpośrednio lub pośrednio. Ustawa nie podaje zamkniętego katalogu danych, które uznaje się za dane osobowe. Podobnie szeroką definicję podaje Naczelny Sąd Administracyjny w jednym ze swoich orzeczeń.

Naczelny Sąd Administracyjny

Dane osobowe to zespół wiadomości (komunikatów) o konkretnym człowieku na tyle zintegrowany, że pozwala na jego zindywidualizowanie*. Obejmuje co najmniej informacje niezbędne do identyfikacji (imię, nazwisko, miejsce zamieszkania), jednakże do tego się nie ogranicza, bowiem mieszczą się w nim również dalsze informacje, wzmacniające stopień identyfikacji (…)* ***O zakwalifikowaniu danej informacji do kategorii danych osobowych decydują przede wszystkim obiektywne kryteria oceny, przy czym uwzględnić należy wszystkie informacje, w tym także pozajęzykowe (kontekst)*** *do jakich dostęp mają osoby trzecie.*

Zamieszczone na stronie Generalnego Inspektora Ochrony Danych Osobowych decyzje, interpretacje i orzeczenia wskazują, że definicja danych osobowych traktowana jest raczej szerzej niż węziej. Okazuje się, że takimi danymi będą nie tylko dane w oczywisty sposób jako takie zakwalifikowane (imię, nazwisko, adres, numer PESEL), ale także dane, co do których można mieć wątpliwości, jak adres e-mail czy IP komputera, z którego łączymy się z internetem. Mając świadomość, jak bardzo nieostre są kryteria traktowania danych jako danych osobowych, zawsze bezpieczniej uznać – nawet na wyrost – jakieś dane za osobowe i chronić je tak starannie, jak to nakazuje ustawa, niż pomylić się w drugą stronę i zaniedbać bezpieczeństwo danych, które mogłyby zostać uznane za dane osobowe przez GIODO lub przez sąd.

Decyzje GIODO

Ustalono, że w procesie przetwarzania danych osobowych, spółka X. jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Postępowaniem administracyjnym, wszczętym z urzędu w celu wyjaśnienia okoliczności sprawy, zostało objęte uchybienie polegające na udostępnianiu bez podstawy prawnej osobom trzecim (użytkownikom internetu zapoznającym się z wpisami dokonanymi na portalu […]) numerów IP komputerów autorów komentarzy wpisywanych na portalu […].

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, wyznaczony w Spółce administrator bezpieczeństwa informacji złożył wyjaśnienia w piśmie z dnia […] stycznia 2010 r., w którym poinformował, że Spółka podjęła decyzję o wprowadzeniu zmian w zakresie publicznego udostępniania adresów IP użytkowników zamieszczających bez rejestracji komentarze na stronach serwisu […]. Zmiana polega na zamaskowaniu części adresu IP na następujących stronach: […], […], […] oraz […], z których nie można dodawać komentarzy do blogów w serwisie. W konsekwencji na stronach serwisu […] nie są aktualnie upubliczniane pełne adresy IP użytkowników zamieszczających komentarze. Jako dowód do ww. pisma załączono wydruki z serwisu internetowego […].

Za: www.giodo.gov.pl

Jak widać z powyższej decyzji, rozpatrując skargę użytkownika na jedną z firm prowadzących portale internetowe, GIODO uznał za dane osobowe adres IP. Założył, że adres IP wystarcza do ustalenia tożsamości osoby pod nim występującej, choć jeden adres IP może być powiązany z więcej niż jedną osobą, jeśli kilka osób korzysta z tego samego połączenia, na przykład w pracy, w domu czy w kawiarence internetowej. Przytaczam tę decyzję nie po to, żeby utrudnić zrozumienie definicji danych osobowych, lecz aby uświadomić, jak bardzo jest ona zależna od kontekstu. Jeśli więc organizacja prowadzi stronę internetową, na której umożliwia zamieszczanie komentarzy niezalogowanym użytkownikom, których IP będzie widoczne dla innych, powinna mieć świadomość, że w podobnym przypadku adres IP znalazł się w kategorii danych osobowych. Dla administratora danych osobowych zawsze lepsza będzie większa ostrożność i traktowanie jako danych osobowych czegoś, co ostatecznie nie zostałoby za dane osobowe uznane, niż podejście odwrotne i przyjęcie dużo węższej definicji danych osobowych.

Zgłaszając do rejestracji zbiór danych osobowych, będziemy musieli wskazać zakres przetwarzanych w nim danych. Katalog ten jest otwarty, ale formularz zgłoszeniowy wymienia najczęściej przetwarzane dane osobowe. Są to:

- imię i nazwisko,
- imiona rodziców,
- data urodzenia,
- miejsce urodzenia,
- adres zamieszkania lub pobytu,
- numer ewidencyjny PESEL,
- Numer Identyfikacji Podatkowej,
- miejsce pracy,
- zawód,
- wykształcenie,
- seria i numer dowodu osobistego,
- numer telefonu.

Nie jest to lista zamknięta, a w zgłoszeniu rejestracyjnym musimy precyzyjnie wskazać zakres przetwarzanych danych. Zapewne nie zbieramy od naszych wolontariuszy, beneficjentów lub darczyńców wszystkich danych osobowych z powyższej listy, ale może są takie, których na niej nie ma, a o które ich prosimy (e-mail, przynależność do organizacji). Stworzenie kompletnej listy danych osobowych gromadzonych przez organizację, wraz z informacją, od kogo są pozyskiwane, jest pierwszym i bardzo ważnym krokiem, gdyż nie wszystkie dane traktowane są tak samo.

Dane osobowe wrażliwe

Szczególną kategorią danych osobowych są tzw. dane wrażliwe, których katalog został wymieniony w art. 27 ustawy. Ustawa nie używa terminu „dane wrażliwe", czasami określane także „danymi sensytywnymi", z języka angielskiego. Jest to termin potoczny, jednakże katalog danych traktowanych jako dane wrażliwe, jest w ustawie wymieniony.

Taki szczególny charakter mają dane ujawniające:

- pochodzenia rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniową, partyjną lub związkową,
- stan zdrowia, kod genetyczny,
- nałogi,
- życie seksualne,
- dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych,
- dane dotyczące innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzając dane wrażliwe, jesteśmy zobowiązani do zapewnienia ich większego bezpieczeństwa, zaś samo przetwarzanie takich danych wiąże się z większymi obostrzeniami.

Przetwarzanie danych osobowych

Ustawa o ochronie danych osobowych

Art. 1 Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.

Dla właściwego zrozumienia zapisów ustawy i obowiązków, jakie na nas nakłada, kluczowa jest sama definicja przetwarzania danych osobowych. Wiele organizacji sądzi, że zbierając podpisy na liście obecności nie przetwarzają danych osobowych, gdyż nic z nimi potem nie robią. Tymczasem ustawowa definicja przetwarzania danych jest bardzo szeroka.

Przetwarzanie danych osobowych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Jak widać z tej definicji, aby przetwarzać dane osobowe, nie trzeba z nimi nic robić, wystarczy je mieć. Jeśli więc w naszym biurze lub na naszym sprzęcie, w formie papierowej lub elektronicznej, znajdują się jakiekolwiek dane osobowe, to już je przetwarzamy, Nawet wtedy, gdy ich nie pozyskaliśmy, gdy znalazły się u nas bez naszej inicjatywy. Fundacje czy stowarzyszenia często dostają listy z prośbą o pomoc i nierzadko taki list zawiera nie tylko dane osobowe, ale również dane wrażliwe, na przykład dotyczące choroby osoby, która prosi o wsparcie. To tylko jeden z przykładów, kiedy możemy niejako niechcący rozpocząć przetwarzanie danych, choć wcale nie mieliśmy takiego zamiaru.

Ustawa o ochronie danych osobowych

Art. 23 Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych,
- jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Powyższe przesłanki są względem siebie równoprawne, co oznacza, że dla legalności procesu przetwarzania danych wystarczające jest spełnienie jednej z nich.

Dużo większe obostrzenia dotyczą przetwarzania danych osobowych wrażliwych. Art. 27 ustawy o ochronie danych osobowych zakazuje przetwarzania takich danych, chyba, że:

1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,

2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,

3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,

5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,.

6) przetwarzanie jest niezbędne do wykonania zadań administratora danych, odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

2

Obowiązki organizacji

Organizacja jako administrator danych osobowych

Administrator danych – organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych.

Organizacja pozarządowa przetwarzająca dane osobowe jest administratorem danych, gdyż decyduje o celach i środkach przetwarzania tych danych. Jako administrator, jest zobowiązana zastosować środki techniczne (zabezpieczenia fizyczna i informatyczne) oraz organizacyjne (struktury i procedury), zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Administrator musi zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz przed zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie. Nie zwalnia go to jednak z odpowiedzialności za przestrzeganie ustawy. Organizacja może w ramach własnej struktury wyznaczyć administratora bezpieczeństwa informacji, ale nie jest to obowiązkowe.

Administrator danych przetwarzając je, powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. W szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub że 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 lub sprostowania danych, do czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub do ich usunięcia ze zbioru.

Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki zapewniające bezpieczeństwo danych. Taka dokumentacja to polityka bezpieczeństwa oraz – w przypadku przetwarzania danych w systemach informatycznych – instrukcja zarządzania systemem informatycznym. Szczegółowe wskazówki opracowywania tych dokumentów znajdują się na internetowej stronie GIODO.

Zbiór danych osobowych

Ustawa o ochronie danych osobowych

Art. 7. Ilekroć w ustawie jest mowa o zbiorze danych osobowych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Pierwszą decyzją, jaką musimy podjąć, jest liczba zgłaszanych zbiorów danych osobowych. Wiele organizacji gromadzi różnego rodzaju dane, w ramach różnych prowadzonych przez siebie działań. Przepisy nie regulują warunków, jakie musi spełniać zbiór danych osobowych, aby można go było uznać za jeden zbiór. Dlatego musimy się tu odwołać do logiki i funkcji zbioru oraz skorzystać z wyjaśnień dostępnych na internetowej stronie Generalnego Inspektora Ochrony Danych Osobowych.

GIODO wyjaśnia

Czy baza danych klientów sklepu internetowego, przetwarzanych w różnych celach, jak np. realizacji zamówień, marketingu, prowadzenia bazy umów cywilnoprawnych, może zostać zgłoszona do rejestracji jako jeden zbiór danych osobowych?

Nie, gdyż dla realizacji różnych celów konieczne będzie przetwarzanie danych osobowych w różnych zakresach, a to oznacza, że zgłoszenie zbioru do rejestracji dotyczy de facto nie jednego, lecz kilku zbiorów prowadzonych w różnych celach.

W rozumieniu ustawy, zbiór danych to „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie" (art. 7 pkt 1 ustawy). Jednocześnie z ustawy o ochronie danych osobowych wynika, iż jedno zgłoszenie zbioru danych powinno obejmować tylko jeden zbiór danych osobowych (art. 41 ustawy). Administrator danych, dokonując zgłoszenia zbioru danych do rejestracji, powinien mieć na uwadze, iż poszczególne zbiory danych osobowych różnią się między sobą m.in. zakresem przetwarzanych danych, celem przetwarzania danych, podstawą prawną prowadzenia zbioru. Dlatego wypełnienie jednego zgłoszenia dla kilku zbiorów danych osobowych, nie pozwala w sposób właściwy scharakteryzować poszczególnych zbiorów objętych tym zgłoszeniem. Tym samym nie można dla każdego z nich wskazać elementów decydujących o jego tożsamości, tj. np. podstawy prawnej przetwarzania danych, zakresu przetwarzanych danych, celu przetwarzania danych w zbiorze, a co za tym idzie, nie jest możliwe stwierdzenie, jaki zakres informacji, o którym mowa w art. 41 ust. 1 ustawy, dotyczy każdego ze zbiorów.

Skoro zatem dane osobowe klientów sklepu internetowego przetwarzane są w różnych celach, jak np. realizacja zamówień klientów sklepu internetowego, prowadzenie statystyk, marketing, prowadzenie bazy umów cywilnoprawnych, to dla ich realizacji potrzebny będzie różny zakres danych osobowych. Prowadzi to do wniosku, że taka baza danych osobowych zawiera faktycznie kilka zbiorów danych, prowadzonych w różnych celach. Dlatego każdy zbiór powinien zostać zgłoszony na oddzielnym formularzu zgłoszeniowym, w którym zostanie uwzględniony odpowiedni zakres danych osobowych oraz cel, dla jakiego są one przetwarzane.

Za: www.giodo.gov.pl

Przykładowe zbiory danych osobowych podlegających rejestracji:

- beneficjenci programów,
- wolontariusze,
- uczestnicy konkursu,
- darczyńcy,
- książka korespondencji.

Zbiory danych osobowych nie podlegające rejestracji:

- zbiory danych dotyczące obecnych i byłych pracowników,
- zbiory danych kandydatów do pracy (podania, itp.).

GIODO wyjaśnia

Czy w GIODO trzeba rejestrować zbiory danych osobowych osób, które wpłaciły 1% podatku na rzecz organizacji pożytku publicznego?

Tak, ale pod warunkiem, że nie zajdzie żadna z przesłanek zwalniających administratora (organizację pożytku publicznego) z obowiązku zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Z zasady organizacje pożytku publicznego zgłaszają do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiory danych osobowych zawierające dane osobowe darczyńców, którzy przekazują na ich rzecz 1 % swojego podatku. Zbiory tego typu podlegają obowiązkowi zgłoszenia do rejestracji, o ile nie zachodzi żadna z przesłanek zwalniających z tego obowiązku, określonych w art. 43 ust. 1 ustawy o ochronie danych osobowych. Może się okazać, że administrator danych osobowych (czyli w tym przypadku organizacja pożytku publicznego) przetwarza dane osobowe w konkretnym zbiorze wyłącznie w celach sprawozdawczości finansowej, w związku z czym nie podlega on obowiązkowi rejestracji na podstawie w art. 43 ust. 1 pkt 8 ustawy o ochronie danych osobowych. Zgodnie bowiem z treścią tego przepisu, z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej. Jeśli jednak zgromadzone dane służą także innym celom, np. wysyłaniu podziękowań, utrzymywaniu kontaktów z darczyńcami, to administrator (organizacja pożytku publicznego) jest zobowiązany zgłosić przedmiotowy zbiór do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Jednocześnie należy wskazać, iż stosownie do postanowień art. 26 ust. 1 ustawy, administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Ta generalna zasada znajduje swoje rozwiniecie w przepisach ustawy określających m.in. wymogi, jakie powinien spełnić administrator w celu zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Jednym z podstawowych obowiązków spoczywających na administratorze jest obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym. Mówi o tym art. 36 ustawy. Wybór środków, jakie zagwarantują przetwarzanym danym optymalny stopień ich zabezpieczenia, pozostawiony został do uznania administratorowi danych. Administrator powinien jednak dysponować takimi instrumentami organizacyjnymi i technicznymi, które zapobiegną nie tylko realnym naruszeniom, ale również możliwości ich powstania. Aby uznać proces przetwarzania danych za zgodny z zasadami ochrony danych osobowych, administrator danych powinien zagwarantować najwyższy stopień zabezpieczenia, tj. wyeliminować wystąpienie szkodliwych zdarzeń, o których mowa w art. 36 ustawy, a gdy jest to niemożliwe – maksymalnie ograniczyć ryzyko ich powstania. W literaturze przedmiotu wyrażono również pogląd, iż „przy stosowaniu zabezpieczeń powinno się uwzględniać też zmieniające się warunki oraz postęp techniczny (informatyczny), co powodować może konieczność zmiany czy modernizowania wprowadzonych wcześniej przez administratora systemów ochrony" (J. Barta, R. Markiewicz, „Ochrona danych osobowych. Komentarz", Zakamycze 2002 r., s. 550). Umożliwieniem dostępu do danych osobie nieupoważnionej będzie więc nie tylko dopuszczenie takiej osoby do urządzeń zawierających dane osobowe, ale także pozostawienie tych urządzeń bez żadnego realnego zabezpieczenia, uniemożliwiającego dostęp do nich. W doktrynie wyrażono stanowisko, iż „przesłanka umożliwienia dostępu nie oznacza tylko czynności nakierowanej na konkretna osobę (osoby) nieuprawnioną, lecz odnosi się także do stworzenia możliwości zapoznania się z danymi osobowymi przez bliżej nieokreślone osoby" (J. Barta, R. Markiewicz, „Ochrona danych osobowych. Komentarz", Zakamycze 2002 r., s. 610).

Ewidencja osób upoważnionych

Administrator danych osobowych nadaje upoważnienia osobom, które w jego imieniu będą przetwarzać dane osobowe i prowadzi ewidencję osób upoważnionych, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej,
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Ustawa nie ogranicza samej formy takiego upoważnienia, zaś GIODO na swojej stronie internetowej informuje, że może mieć ono nawet formę maila służbowego, pod warunkiem, że zawiera on wymienione powyżej dane, wymagane ustawą.

Osoby, które zostały upoważnione do przetwarzania danych, są zobowiązane do zachowania w tajemnicy zarówno samych danych jak i sposobów ich zabezpieczenia.

Obowiązek informacyjny

Organizacja pozyskująca dane osobowe ma, wobec osób, od których je zbiera, tzw. „obowiązek informacyjny". Prosząc osobę fizyczną o zgodę na przetwarzanie jej danych osobowych, administrator musi poinformować ją o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Zazwyczaj powyższe informacje są częścią formuły zgody na przetwarzanie danych osobowych, która może brzmieć na przykład:

„Wyrażam zgodę na przetwarzanie moich danych osobowych przez Fundację Rozwoju Społeczeństwa Obywatelskiego z siedzibą w Warszawie, ul. Kłopotowskiego 6 m 59/60 dla celów związanych z realizacją programu „Fimango – zarządzanie finansami w organizacjach pozarządowych". Podanie danych jest dobrowolne. Przysługuje mi prawo dostępu do treści moich danych oraz do ich poprawienia."

Po kontroli GIODO

Na podstawie zgromadzonego materiału dowodowego ustalono, że Fundacja „XYZ", jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Nieinformowaniu osób adoptujących zwierzęta, o prawie dostępu do treści swoich danych oraz ich poprawiania, a także o dobrowolności podania danych (art. 24 ust. 1 pkt 3 i pkt 4 ustawy).

2. Niedopełnieniu obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy, w stosunku do osób, których dane osobowe zostały włączone do zbioru danych osób adoptujących zwierzęta prowadzonego przez Fundację.

W toku czynności kontrolnych ustalono, iż osoby adoptujące zwierzęta nie są informowane przez Fundację o prawie dostępu do treści swoich danych oraz ich poprawiania, a także o dobrowolności podania danych. Zgodnie z art. 25 ust. 1 ustawy, w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, 3) źródle danych, 4) prawie dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8. Jak ustalono w toku kontroli, Fundacja przechowuje umowy adopcyjne, które zostały zawarte z właścicielami zwierząt jeszcze przed utworzeniem Fundacji przez osobę, która obecnie jest Prezesem Fundacji. Natomiast jak ustalono w toku kontroli, po włączeniu danych osób, o których mowa powyżej, do zbioru obecnie prowadzonego przez Fundację, nie został dopełniony obowiązek informacyjny wobec tych osób, w zakresie, o którym mowa w art. 25 ust. 1 ustawy.

Zgoda na przetwarzanie danych

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

Ustawodawca nałożył na przetwarzających dane obowiązek uzyskania zgody osoby, której dane mają być przetwarzane, na takie przetwarzanie. Jeśli więc chcemy na przykład zbierać dane osób, które wzięły udział w prowadzonych przez nas warsztatach, musimy uzyskać od nich zgodę na przetwarzanie ich danych. Jest to konieczne nawet wówczas, gdy jedyne co zamierzamy z tymi danymi robić, to trzymać je w archiwum. Wiele organizacji błędnie przyjmuje, że ktoś, kto się dobrowolnie zgłosił i podpisał na liście, wyraził tym samym zgodę na przetwarzanie swoich danych osobowych (a pamiętajmy – przetwarzaniem danych w rozumieniu ustawy jest także ich przechowywanie!).

Z definicji zgody, ani z innych zapisów ustawy, nie wynikają szczegółowe zasady formułowania zgody. Podkreśla się jednak, że z treści zgody na przetwarzanie danych osobowych powinno w sposób nie budzący 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. Bardzo często formuły zgody na przetwarzanie danych osobowych, jakie przychodzi nam wypełniać, sformułowane są wadliwie. Czasami nie zawierają wszystkich niezbędnych informacji, a czasami zawierają zapisy uznane przez Urząd Ochrony Konkurencji i Konsumenta za tzw. „klauzule niedozwolone". W Rejestrze klauzul niedozwolonych, który prowadzi UOKiK, znajduje się kilka przykładów formułek nie spełniających ustawowych wymogów.

Przykłady klauzul niedozwolonych

*„**Równocześnie** uczestnik wyraża zgodę na przetwarzanie i przekazywanie swoich danych osobowych **innym instytucjom**. Dane osobowe podawane są dobrowolnie, jednak są niezbędne do zawarcia umowy."*

„Posiadacz Konta (...) wyraża zgodę na zamieszczenie i przetwarzanie swoich danych osobowych w bazie danych osobowych Banku dla celów promocyjnych i marketingowych Banku, podmiotów z nim współpracujących w zakresie świadczonych przez Bank usług bankowych oraz innych podmiotów, z którymi Bank współpracuje przy sprzedaży ich produktów i usług, a także na otrzymywanie informacji handlowej np.: o świadczonych usługach i oferowanych produktach, propozycji udziału w promocjach."

„Posiadacz Konta oświadcza, że: został poinformowany o przetwarzaniu przez Bank oraz podmioty związane z Bankiem umową o współpracy w zakresie świadczonych usług bankowych, swoich danych osobowych oraz danych o wierzytelnościach i zobowiązaniach uzyskanych w wyniku zawarcia niniejszej umowy, w celu należytego jej wykonywania oraz realizacji innych celów statutowych Banku, w tym również po wygaśnięciu niniejszej umowy."

„Zainteresowany wyraża zgodę na udostępnienie swoich danych osobowych przekazanych pośrednikowi w celu opracowania niniejszej umowy. Dalej wyraża zgodę na przechowywanie i przetwarzanie jego danych osobowych oraz wykorzystywanie ich przez pośrednika lub osobę trzecią w celu składania ofert handlowych lub oferowania usług na czas nieokreślony zgodnie z ustawą o ochronie danych osobowych."

„Zainteresowany wyraża zgodę na udostępnienie swoich danych osobowych oraz wyraża zgodę na przechowywanie, przetwarzanie, przekazywanie i wykorzystanie jego danych osobowych w celu przewidzianym umową, marketingowym i reklamowym przez pośrednika, wierzyciela i osoby trzecie. Pośrednik będzie postępować z danymi osobowymi zainteresowanego zgodnie z obowiązującymi przepisami, a w szczególności zgodnie z ustawą o ochronie danych osobowych."

„Podpisując umowę – zgłoszenie uczestnictwa, wyrażają jednocześnie Państwo zgodę na przetwarzanie, uaktualnianie i udostępnianie swoich danych osobowych, niezbędnych dla realizacji imprezy oraz dla celów promocyjnych Biura (zgodnie z art. 23 pkt. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.)."

„Podpis pod warunkami ogólnymi umowy jest równoznaczny z wyrażeniem zgody na przetwarzanie danych osobowych w bazie danych AICE oraz na przekazywanie innym podmiotom, w tym firmom ubezpieczeniowym w usprawiedliwionych celach wynikających z umowy, a także na zamieszczanie w prasie wyników asygnacji (nazwisko, imię, miejscowość)."

Decyzje GIODO

Do Biura GIODO wpłynęło pismo, do którego załączony został formularz zamówienia egzemplarza książki „Fatima – orędzie tragedii czy nadziei!". Z treści przesłanego pisma wynikało, iż Fundacja uzależnia realizację zamówienia na oferowane do sprzedaży produkty od podpisania przez zamawiających klauzuli o następującej treści: „wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w niniejszym kuponie przez Fundację (...), w celach statutowych Fundacji oraz na ich udostępnienie podmiotom prowadzącym podobną działalność. Administratorem Państwa danych osobowych jest Fundacja (...). Państwa dane są zbierane w celu ich przetwarzania przez Fundację w związku z realizacją jej zadań statutowych. Dane mogą być udostępniane innym podmiotom, zwłaszcza Fundacjom i stowarzyszeniom, które prowadzą podobną działalność. Fundacja informuje, że przysługuje Państwu prawo wglądu i korekty swoich danych oraz prawo żądania ich usunięcia ze zbioru danych".

W złożonych wyjaśnieniach wskazano ponadto, iż podmiot, któremu są udostępniane dane osobowe, tj. Stowarzyszenie Z (odbiorca danych), zwane dalej Stowarzyszeniem, realizuje podobne co Fundacja zadania statutowe i cele.

Po przeprowadzeniu postępowania administracyjnego w przedmiotowej sprawie, Generalny Inspektor Ochrony Danych Osobowych w dniu 28 października 2004 r. wydał decyzję administracyjną (znak: GI-DEC-DS-231/04/493), w której nakazał Fundacji, usunięcie uchybień w procesie przetwarzania danych osobowych osób zamawiających oferowane przez nią produkty, pozyskanych za pomocą formularza zamówienia, poprzez odbieranie od nich odrębnej zgody na udostępnienie innym podmiotom dotyczących ich danych osobowych.

Generalny Inspektor w pełni podtrzymuje stanowisko, iż analiza stanu faktycznego i prawnego niniejszej sprawy daje podstawy do przyjęcia stanowiska, iż jedyną przesłanką umożliwiającą Fundacji udostępnianie innym podmiotom danych osobowych pozyskanych przez Fundację z formularzy zamówień określonych produktów, jest wyraźna zgoda na powyższą czynność osób, których dane te dotyczą. Należy bowiem wyraźnie podkreślić, iż każdej osobie, której dane dotyczą, przysługuje prawo do decydowania o tym, komu oraz w jakich okolicznościach jej dane osobowe zostaną w przyszłości udostępnione. W przedmiotowej sprawie, Fundacja, stosując formularz nie zawierający odrębnej zgody na udostępnianie danych innym podmiotom, pozbawia osoby zamawiające jej produkty powyższego uprawnienia. Jednostronnie bowiem wymusza od osób zamawiających w Fundacji oferowane do sprzedaży produkty zaakceptowanie sytuacji, w której ich dane zostaną przekazane nieograniczonej liczbie podmiotów.

Działanie to w konsekwencji uniemożliwia tym osobom skuteczną kontrolę procesu przetwarzania ich danych osobowych. Z dotychczasowego brzmienia formularza zamówienia produktów wynika, że każda osoba, która chce wejść w posiadanie produktów Fundacji i składa w tym zakresie zamówienie, automatycznie godzi się na przekazanie jej danych innym podmiotom. Natomiast, w myśl art. 7 pkt 5 ustawy, poprzez zgodę na przetwarzanie danych osobowych, należy rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści

Warto również zwrócić uwagę, iż stanowisko Generalnego Inspektora znajduje potwierdzenie zarówno w doktrynie, jak również w orzecznictwie Naczelnego Sądu Administracyjnego. W literaturze przedmiotu prezentowany jest pogląd, iż „jeśli oświadczenie woli o wyrażaniu zgody na przetwarzanie danych nie obejmowało możliwości udostępnienia danych innemu ⇨

administratorowi, działanie takie jest niedopuszczalne, dla udostępnienia danych innym podmiotom konieczna jest dodatkowa zgoda osoby, której dane dotyczą (Janusz Barta, Ryszard Markiewicz Ochrona danych osobowych Komentarz, Zakamycze 2002 s. 388, S. Grynhoff i P. Woźny „Ochrona Danych Osobowych w praktyce" pkt 2/2, s. 7-11, podobnie Fleszer D. „Prawo do kontroli przetwarzania swoich danych osobowych artykuł" P Glosa 2004/1/17 – t.3).

Zauważyć również należy, iż w podobnej sprawie Naczelny Sąd Administracyjny wskazał w wyroku z dnia 4 kwietnia 2003 r., iż „zgoda na przekazywanie danych musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych". W uzasadnieniu do przedmiotowego wyroku stwierdzono ponadto, iż „zdaniem Sądu, o ile można uznać za taką umowę nienazwaną kupno książek za pośrednictwem Spółki, o tyle odrębną kwestią jest umowa o przekazanie danych osobowych. Przekazanie danych jest sprawą odrębną od życia codziennego, a obie te umowy nie są tożsame. Skład orzekający zaakcentował bardziej rygorystyczne wymogi wprowadzone przez ustawodawcę w odniesieniu do zgody na przekazywanie danych osobowych wyrażone z art. 7 pkt 5 ustawy. Oznacza to zdaniem Sądu, że wyrażający zgodę musi mieć w momencie jej zawierania świadomość tego, co kryje się pod tym pojęciem" (Wyrok Naczelnego Sądu Administracyjnego z dnia 4 kwietnia 2003 r. II SA 2135/2002 Monitor Prawniczy 2003/10 str. 435, podobnie wyrok NSA z dnia 19 listopada 2001 r. II S.A. 2748/00).

Z powyższego wynika zatem jednoznacznie, iż działanie Fundacji, polegające na przekazywaniu danych osób zamawiających produkty w Fundacji innym pomiotom, nie naruszałoby przepisów ustawy wówczas, gdyby osoby, których dane dotyczą, bezsprzecznie wyraziły zgodę na przeprowadzenie takich działań we wskazanym powyżej celu. Ponadto osoby, których dane dotyczą, powinny być świadome dobrowolności, bądź konieczności złożenia oświadczenia, którego treścią jest taka zgoda. Dlatego też zgoda na przetwarzanie danych osobowych tego, kto je składa, powinna być przedmiotem odrębnego oświadczenia, niezależnego od oświadczenia stanowiącego akceptację zamówienia.

Za: www.giodo.gov.pl

Kontrola GIODO

Organem powołanym do czuwania nad realizacją przepisów o ochronie danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych, którego pracownicy mają prawo przeprowadzania kontroli w instytucjach i w organizacjach. Kontrolę przeprowadzają inspektorzy, na podstawie imiennego upoważnienia, które każdorazowo określa, co jest poddawane kontroli. Może to być organizacja (w celu sprawdzenia, czy przetwarza dane osobowe i czy robi to zgodnie z prawem), albo zgłoszony przez nią konkretny zbiór danych osobowych (w celu sprawdzenia poprawności przetwarzania gromadzonych w nim danych), albo samo miejsce (w celu sprawdzenia, czy znajdują się w nim podlegające ustawie dane osobowe, a jeśli tak – czy są przetwarzane zgodnie z prawem). Upoważnienie zawiera także termin przeprowadzenia kontroli, wyznaczając jej początek oraz wskazując przewidywany koniec (ten jednak może oczywiście ulec przedłużeniu).

Kontrolerzy mają prawo, na podstawie legitymacji służbowej oraz imiennego upoważnienia do przeprowadzenia kontroli, do inspekcji (w godzinach 6.00-

22.00) pomieszczeń, w których przetwarzane są dane osobowe. Mogą także przeprowadzać niezbędne czynności kontrolne o różnym charakterze, np. prosić o okazanie zawartości szuflad, szaf, segregatorów, itp. W trakcie kontroli mogą także żądać wyjaśnień (pisemnych lub ustnych) oraz wzywać i przesłuchiwać osoby, jeśli będzie to konieczne dla ustalenia faktów. Kontrolerzy mają też prawo wglądu do dokumentów i do ich kopiowania. Mogą również dokonywać oględzin urządzeń (np. komputerów), nośników (np. dysków, na których przechowujemy dane) oraz systemów informatycznych.

Po zakończeniu kontroli, zespół kontrolujący sporządza protokół pokontrolny, który przekazuje kontrolowanej organizacji. Protokół, oprócz danych dotyczących samej kontroli, zawiera także opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje o istotnym znaczeniu dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi. W razie odmowy podpisania protokołu przez kontrolowanego administratora danych, inspektor zaznacza to w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi.

Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o wydanie decyzji administracyjnej nakazującej przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień,
2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
4) wstrzymanie przekazywania danych osobowych do państwa trzeciego,
5) zabezpieczenie danych lub przekazanie ich innym podmiotom,
6) usunięcie danych osobowych.

Jeśli kontrolowana organizacja nie zgadza się z wydaną decyzją, może zwrócić się do Generalnego Inspektora z wnioskiem o ponowne rozpatrzenie sprawy. Przysługuje jej też skarga do sądu administracyjnego, bowiem to właśnie Kodeksu postępowania administracyjnego reguluje procedury odwoławcze.

W przypadku poważniejszych naruszeń, inspektor może żądać wszczęcia postępowania dyscyplinarnego przeciwko osobom winnym uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i o podjętych działaniach. W razie stwierdzenia, że działanie lub zaniechanie zarządu organizacji lub jej pracownika odpowiedzialnego z ochronę danych osobowych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do prokuratury zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

3

Zgłaszanie zbiorów danych osobowych

Organizacja, która jest administratorem danych osobowych podlegających rejestracji, musi zgłosić zbiór lub zbiory danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych. Z takiego obowiązku zwolnieni są administratorzy niektórych rodzajów zbiorów danych. Organizacja nie musi na przykład zgłaszać zbioru danych osobowych:

- swoich pracowników etatowych i zatrudnianych na umowy cywilnoprawne,
- swoich członków,
- swoich klientów, jeśli są pozyskiwane wyłącznie w celu wystawienia rachunku, faktury lub prowadzenia sprawozdawczości finansowej,
- osób podpisujących listy poparcia pod wnioskiem o referendum lokalne lub ogólnokrajowe,
- osób korzystających z ich usług medycznych,
- danych powszechnie dostępnych,
- danych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Obowiązek zgłaszania Generalnemu Inspektorowi dotyczy też każdej zmiany informacji podanych we wcześniejszym zgłoszeniu, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. Jeżeli zmiana informacji dotyczy rozszerzenia zakresu przetwarzanych danych o dane wrażliwe, administrator danych jest obowiązany do jej zgłoszenia przed dokonaniem zmiany w zbiorze.

Zgłoszenia dokonuje się na formularzu według ustalonego wzoru, który przedstawiamy w załącznikach.

Organizacja dysponująca bezpiecznym podpisem elektronicznym, może zgłosić zbiór przez Internet, poprzez specjalnie do tego celu uruchomioną platformę internetową (www.egiodo.gov.pl). Na platformie można też przejrzeć bazę zarejestrowanych zbiorów danych osobowych, wyszukiwanych według nazwy czy siedziby administratora danych. Udostępniona przez platformę aplikacja wspiera prawidłowe wypełnianie zgłoszenia zbioru danych do rejestracji, wymuszając

podanie wszystkich wymaganych przepisami informacji. Dzięki temu możemy mieć pewność, że zgłoszenie, które wyślemy, będzie przynajmniej kompletne (program nie ma możliwości weryfikowania prawidłowości podanych danych). Wypełniony na platformie formularz, można podpisać bezpiecznym podpisem elektronicznym i wysłać bezpośrednio ze strony GIODO lub wydrukować i przesłać pocztą tradycyjną.

Załączniki

W tym rozdziale znajdziesz kompletny formularz zgłoszenia zbioru danych osobowych, wraz z komentarzami do każdej rubryki.

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI
GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

* ☐ – zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285),

Komentarz: *To okienko zaznaczasz, jeśli* ***dokonujesz zgłoszenia*** *zbioru danych osobowych, a* ***zbiór nie zawiera danych wrażliwych****, tj. danych „ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym". Jeśli masz wątpliwości, które okienko zaznaczyć, przejdź do punktu 9 i sprawdź, czy zaznaczysz którąkolwiek z opcji.*

* ☐ – zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

Komentarz: *To okienko zaznaczasz, jeśli zgłoszenie dotyczy zbioru danych osobowych już wcześniej zarejestrowanego, do którego chcesz zgłosić zmiany dotyczące:*
– oznaczenia organizacji prowadzącej zbiór, adresu jej siedziby, numeru REGON,
– podstawy prawnej upoważniającej do prowadzenia zbioru,
– celu przetwarzania danych,
– opisu kategorii osób, których dane dotyczą,
– zakresu przetwarzanych danych,
– sposobu zbierania oraz udostępniania danych,
– odbiorców, którym dane mogą być przekazywane,
– środków technicznych i organizacyjnych zastosowanych w celu zapewnienia bezpieczeństwa danych,
– ewentualnego przekazywania danych do państwa trzeciego.
Na zgłoszenie zmian dotyczących zbioru danych osobowych masz 30 dni, licząc od dnia dokonania zmiany w zbiorze danych. Jeżeli natomiast zgłaszana zmiana informacji dotyczy rozszerzenia zakresu przetwarzanych danych o dane wrażliwe, zgłoszenia aktualizacyjnego należy dokonać przed dokonaniem zmiany w zbiorze.

* ☐ – zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Komentarz: *To okienko zaznaczasz, jeśli w zbiorze, który chcesz zarejestrować, będą przetwarzane dane wrażliwe, tj. dane „ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym". Jeśli masz wątpliwości, które okienko zaznaczyć, przejdź do punktu 9 i sprawdź czy zaznaczysz którąkolwiek z opcji.*

Nr .....
(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

Przykład: *„Wolontariusze Fundacji XYZ”*

do Rejestru Zbiorów Danych Osobowych.

Komentarz: *Nazwę zbioru danych osobowych nadaje sam administrator, czyli organizacja dokonująca rejestracji zbioru. Ustawa nie precyzuje zasad nazewnictwa, dobrze, by nazwa była zwięzła i oddająca charakter zgromadzonych w zbiorze danych. Jeden formularz dotyczy zawsze tylko jednego zbioru danych. Jeśli więc organizacja gromadzi dane wolontariuszy, beneficjentów, darczyńców – a zatem grup, w przypadku których różny jest zakres gromadzonych danych, cele ich przetwarzania, zasady udostępniania – powinna zarejestrować te zbiory osobno. Nie ma ograniczeń liczby zbiorów danych osobowych prowadzonych przez jedną organizację.*

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

Należy wpisać dane organizacji zgłaszającej zbiór.

(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel Wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

Nie dotyczy organizacji mających siedzibę w Polsce.

(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:

Komentarz: *Ten punkt wypełniamy tylko wtedy, gdy organizacja (administrator danych) powierza lub przewiduje powierzenie przetwarzania danych innemu podmiotowi. Możliwość powierzenia przetwarzania danych innemu podmiotowi przewiduje art. 31 ustawy o ochronie danych osobowych, umowa powierzenia przetwarzania danych osobowych musi mieć formę pisemną, a podmiot, któremu powierzono przetwarzanie danych osobowych może to robić wyłącznie w celu i w zakresie określonym w umowie. W przypadku powierzenia przetwarzania danych innemu podmiotowi, odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze, co nie wyłącza odpowiedzialności podmiotu, któremu przetwarzanie danych zostało powierzone, w przypadku przetwarzania ich niezgodnie z zawartą umową.*

* ☐ – administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),

* ☐ – administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

W przypadku powierzenia przetwarzania danych innemu podmiotowi, podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

.....

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

Komentarz: *W tym punkcie należy zakreślić właściwe pole (lub pola), wskazujące podstawę prawną przetwarzania danych w tym zbiorze. Zgodnie z art. 23 ustawy o ochronie danych osobowych, przetwarzanie danych osobowych jest dopuszczalne, gdy:*

- *osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,*
- *jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,*
- *jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,*
- *jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,*
- *jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.*

* ☐ – zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,

Komentarz: *Najczęściej podstawą przetwarzania danych osobowych przez organizacje pozarządowe jest zgoda osób, których dane przetwarzamy – wolontariuszy, beneficjentów, stypendystów, darczyńców, partnerów. Zgodnie z art. 7 ustawy o ochronie danych osobowych, zgoda taka to „oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie". Zgoda może obejmować nie tylko przetwarzanie danych w czasie jej pozyskiwania, ale również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a pozyskanie od niej zgody jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe*.

* ☐ – przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa

Komentarz: *Zaznaczając ten punkt, musimy precyzyjnie określić przepisy prawa, które zezwalają na przetwarzanie danych osobowych, wskazując tytuł oraz miejsce publikacji aktu prawnego. Najczęściej wskazywane przepisy to:*

– Ustawa z dnia 7 września 1991 r. o systemie oświaty,
– Ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej,
– Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym,
– Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego,
– Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych,
– Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi,
– Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej,
– Ustawa z dnia 12 marca 2004 r. o pomocy społecznej.

* ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

* ☐ – przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego – jeśli TAK, to opisz te zadania:

Komentarz: *Zaznaczenie tego punktu wymaga wymienienia „określonych prawem zadań realizowanych dla dobra publicznego" i będących zdaniem administratora danych podstawą prawną do przetwarzania przez niego tych danych*.

* ☐ *ew. cd. w załączniku nr*

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

Komentarz: *Zaznaczając ten punkt nie musimy podawać żadnych dodatkowych danych. Art. 23 ustawy o ochronie danych osobowych wymienia dwa przykładowe „prawnie usprawiedliwione cele":*
– marketing bezpośredni własnych produktów lub usług administratora danych,
– dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

Komentarz. *Należy wskazać precyzyjny i konkretny cel przetwarzania danych w zgłaszanym do rejestracji zbiorze*.

..... * ☐ *ew. cd. w załączniku nr*

6. Opis kategorii osób, których dane dotyczą:

Komentarz: *Należy wskazać, jakich kategorii osób dotyczą dane przetwarzane w zbiorze, np. „klienci", „darczyńcy", „wnioskodawcy".*

7. Zakres przetwarzanych w zbiorze danych o osobach:

Komentarz: *W tym punkcie należy zaznaczyć rodzaje gromadzonych w zgłaszanym zbiorze danych. Wypełniając ten punkt, warto wziąć pod uwagę wszystkie dane, jakie docelowo będziemy zbierać, żeby uniknąć konieczności aktualizowania zgłoszenia, gdy zechcemy rozszerzyć rodzaj zbieranych danych*.

* ☐ – nazwiska i imiona,	* ☐ – Numer Identyfikacji Podatkowej,
* ☐ – imiona rodziców,	* ☐ – miejsce pracy,
* ☐ – data urodzenia,	* ☐ – zawód,
* ☐ – miejsce urodzenia,	* ☐ – wykształcenie,
* ☐ – adres zamieszkania lub pobytu,	* ☐ – seria i numer dowodu osobistego,
* ☐ – numer ewidencyjny PESEL,	* ☐ – numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt 7, przetwarzane w zbiorze – *należy podać, jakie*:

Komentarz: *W tym miejscu należy wpisać inne dane przetwarzane w zgłaszanym zbiorze, niewymienione na liście w punkcie 7, i niebędące danymi wrażliwymi, wymienionymi w punkcie 9*.

..... * ☐ *ew. cd. w załączniku nr*

9. Dane przetwarzane w zbiorze:

Komentarz: *Punkty 9 i 10 dotyczą pozyskiwania tzw. danych wrażliwych, których przetwarzanie wiąże się dla organizacji z dodatkowymi obowiązkami. Dane takie muszą być bardziej chronione, a ich przetwarzanie ma szereg ograniczeń.*

Jeśli zaznaczyliśmy choć jedną opcję w punkcie 9, zgłoszenie wypełniane na platformie eGIODO automatycznie zmieni kategorię naszego wniosku. Jeśli natomiast wypełniamy wniosek w wersji papierowej, musimy sprawdzić, czy prawidłowo wskazaliśmy rodzaj zgłoszenia (pierwsze rubryki formularza) – zgłoszenie wypełnione w punkcie 9 musi być oznaczone jako „zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.”.

a) ujawniają 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,

b) dotyczą:

* ☐ – skazań,
* ☐ – mandatów karnych,
* ☐ – orzeczeń o ukaraniu,
* ☐ – innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść od razu do pkt 11.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

* ☐ – osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,
* ☐ – przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych – jeśli TAK, to podaj odniesienie do przepisu tej ustawy:

Komentarz: *Należy wskazać odniesienie do szczególnego przepisu innej ustawy zezwalającej na przetwarzanie danych wskazanych w pkt 9, bez zgody osoby, której te dane dotyczą. Przykładowe ustawy*:

– Ustawa z dnia 7 września 1991 r. o systemie oświaty,
– Ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej,
– Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym,
– Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego,
– Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych,
– Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi,
– Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej,
– Ustawa z dnia 12 marca 2004 r. o pomocy społecznej.

* ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

* ☐ – przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych – jeśli TAK, to podaj, jakich:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

* ☐ – przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

* ☐ – przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

* ☐ – przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

* ☐ – przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,

* ☐ – przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Sposób zbierania danych do zbioru:

Komentarz: *Należy wskazać źródło pozyskiwania danych. W przypadku, jeżeli dane będą pozyskiwane zarówno od osób, których dotyczą jak i z innych źródeł, wówczas należy zaznaczyć obydwa wymienione w tym punkcie pola wyboru*.

* ☐ – od osób, których dotyczą,

* ☐ – z innych źródeł niż osoba, której dane dotyczą,

12. Sposób udostępniania danych ze zbioru:

Komentarz: *Należy zaznaczyć pole wyboru, jeżeli pozyskane dane będziemy przekazywać podmiotom innym niż uprawnione do ich pozyskania na podstawie obowiązujących przepisów prawa*.

* ☐ – podmiotom innym niż upoważnione na podstawie przepisów prawa,

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane – należy *podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu dane mogą być przekazywane:*

Komentarz: *Należy wymienić wszystkich odbiorców lub kategorie odbiorców, którym dane mogą być przekazywane. W rozumieniu ustawy odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyjątkiem:*
– *osoby, której dane dotyczą,*
– *osoby upoważnionej do przetwarzania danych,*
– *organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem*.

* ☐ *ew. cd. w załączniku nr*

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego – *podaj nazwę państwa:*

Komentarz: *Państwo trzecie to państwo nie należące do Europejskiego Obszaru Gospodarczego. Należy podać nazwę państwa, do którego będą przekazywane dane osobowe, pamiętając, że osoba, której dane będą przekazane, musi wyrazić na to zgodę na piśmie*.

* ☐ *ew. cd. w załączniku nr*

Część E. Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(w poniższych odpowiedziach proszę nie ujawniać szczegółów zastosowanych rozwiązań)

15. Zbiór danych osobowych będzie przetwarzany:

Komentarz: *Należy zaznaczyć jedną z dwóch możliwości przetwarzania danych*.

a) * ☐ – centralnie

Komentarz: *Centralne prowadzenie zbioru danych, zarówno w przypadku przetwa-rzania danych w systemie informatycznym, jak i systemie papierowym, oznacza zlokalizowanie danych w jednym miejscu. Zbiór prowadzony jest centralnie w sytuacji zgromadzenia danych (zarówno w postaci papierowej jak i zamieszczo-nych na serwerze) w jednym pomieszczeniu lub budynku*.

* ☐ – w architekturze rozproszonej

Komentarz: *Prowadzenie zbioru w architekturze rozproszonej, zarówno w przypadku przetwarzania danych w systemie informatycznym, jak i w systemie papierowym, oznacza, że dane są przetwarzane w sposób zdecentralizwany. Zbiór prowadzony jest w architekturze rozproszonej (w przypadku przetwarzania danych w systemie informatycznym) np. w sytuacji gromadzenia danych na dwóch serwerach zlokalizowanych w odrębnych budynkach*.

b) * ☐ – wyłącznie w postaci papierowej

* ☐ – z użyciem systemu informatycznego

c) * ☐ – z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych, połączonego z siecią publiczną (np. Internetem),

Komentarz: *System używany do przetwarzania danych osobowych jest połączony z siecią publiczną jeżeli co najmniej jedno urządzenie (komputer, router, modem) będące jego częścią, jest połączone z siecią publiczną tzn. z siecią telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800 z późn. zm.). Zaznaczenie tej opcji wiąże się w koniecznością wykazania większej liczby zabezpieczeń*.

* ☐ – bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych, połączonego z siecią publiczną (np. Internetem),

16. Zostały spełnione wymogi określone w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)]:

Komentarz: *Artykuły od 36 do 39 ustawy o ochronie danych osobowych wymieniają wymogi, jakie należy spełnić przetwarzając dane osobowe. Administrator danych osobowych, czyli organizacja zgłaszająca zbiór do rejestracji, może je wykonywać osobiście lub wyznaczyć administratora bezpieczeństwa informacji, który w jej imieniu nadzoruje przestrzeganie zasad ochrony danych osobowych.*

Administrator danych osobowych ma obowiązek:

– *zastosować środki techniczne (zabezpieczenia fizyczne i informatyczne) i organizacyjne (struktury i procedury) zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz do 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,*

– *prowadzić dokumentację opisującą sposób przetwarzania danych oraz wymienione powyżej środki techniczne i organizacyjne – to jest politykę bezpieczeństwa, a jeśli dane przetwarzane są w systemie informatycznym, to także instrukcję zarządzania tym systemem.*

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych, który ma obowiązek zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej,

2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

a) * ☐ – został wyznaczony administrator bezpieczeństwa informacji, nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych,

Komentarz: *Punkt nieobowiązkowy, administrator danych może sam wykonywać czynności administratora bezpieczeństwa informacji.*

* ☐ – administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

Komentarz: *Punkt należy zaznaczyć, jeśli nie został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad przetwarzania danych osobowych.*

b) * ☐ – do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,

Komentarz*: Punkt obowiązkowy.*

c) * ☐ – prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

Komentarz: *Punkt obowiązkowy.*

d) * ☐ – została opracowana i wdrożona polityka bezpieczeństwa.

Komentarz: *Punkt obowiązkowy.*

e) * ☐ – została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,

Komentarz: *Punkt obowiązkowy jeśli w punkcie 15b zaznaczyliśmy, że dane będą przetwarzane z użyciem systemu informatycznego.*

f) Inne środki, oprócz wymienionych w pkt. a – e, zastosowane w celu zabezpieczenia danych:

Komentarz: *W tym punkcie możemy wpisać dodatkowe środki bezpieczeństwa wprowadzone w organizacji w celu ochrony przetwarzanych przez nią danych osobowych. W formularzu na platformie eGIODO możemy wybrać, na przykład:*

Środki ochrony technicznej:
– Drzwi (zwykłe, o podwyższonej odporności ogniowej, o podwyższonej odporności na włamanie)
– Kraty, rolety lub folia antywłamaniowa.
– System alarmowy przeciwwłamaniowy.
– System kontroli dostępu, monitoring z zastosowaniem kamer przemysłowych, lub ochrony.
– Szafa zamknięta (niemetalowa, metalowa, sejf).
– System przeciwpożarowy i/lub wolnostojąca gaśnica.
– Niszczarki dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
– Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
– Urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
– Zabezpieczenie systemu przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
– Zabezpieczenie za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
– Środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych..
– Systemowe mechanizmy wymuszające okresową zmianę haseł.
– System rejestracji dostępu do systemu/zbioru danych osobowych.
– Środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
– Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
– Środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie.
– System Firewall lub IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych:
– Środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
– Środki umożliwiające określenie praw dostępu do wskazanego zakresu danych.
– Dostęp z uwierzytelnieniem z wykorzystaniem identyfikatora użytkownika oraz hasła.
– Mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
– Kryptograficzne środki ochrony danych osobowych.
– Wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
– Mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Środki organizacyjne:
– Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
– Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
– Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
– Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane osobom postronnym.
– Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 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)

17. Zastosowano środki bezpieczeństwa na poziomie:

Komentarz: *Ten punkt wypełniamy tylko wówczas, gdy w punkcie 15b zaznaczyliśmy przetwarzanie danych osobowych z wykorzystaniem systemu informatycznego*.

* ☐ – podstawowym,

Komentarz: *Zaznaczamy tylko wtedy, gdy w zgłaszanym zbiorze nie będą przetwarzane dane wrażliwe, a żadne z urządzeń służących do przetwarzania danych nie jest połączone z publiczną siecią teleinformatyczną.*

* ☐ – podwyższonym,

Komentarz: *Zaznaczamy, jeśli w zgłaszanym zbiorze będą przetwarzane dane wrażliwe, ale żadne z urządzeń służących do przetwarzania danych nie jest połączone z publiczną siecią teleinformatyczną.*

* ☐ – wysokim.

Komentarz: *Zaznaczamy zawsze, jeśli choć jedno z urządzeń służących do przetwarzania danych jest połączone z publiczną siecią teleinformatyczną.*

.....

(data, podpis i pieczęć wnioskodawcy)

Objaśnienia:

* W przypadku odpowiedzi twierdzącej, należy zakreślić kwadrat lilerą „X".

1) Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym), zobowiązany jest do zastosowariia środków określonych w pkt 15 ppkt a – d, a w przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 16 ppkt e.

2) Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 ww. rozporządzenia (UWAGA! Dotyczy wyłącznie administratorów przetwarzających dane w systemie informatycznym):

– jeżeli wnioskodawca przetwarza dane wymienione w pkt 9 zgłoszenia, należy zastosować środki bezpieczeństwa przynajmniej na poziomie podwyższonym;

– w przypadku, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną, należy stosować środki bezpieczeństwa na poziomie wysokim;

– w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym.

Zgłoszenia można dokonać drogą elektroniczną, za pomocą programu komputerowego umożliwiającego jego prawidłowe wypełnienie, dostępnego na stronie intenetowej Generalnego Inspektora Ochrony Danych Osobowych.