

**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 z późn. zm.),
- * zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
- * zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr

(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

do Rejestru Zbiorów Danych Osobowych

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

Administrator: REGON: Miejscowość: Kod pocztowy: Ulica: Nr domu: Lokal:

(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:

Przedstawiciel:

Miejscowość: Kod pocztowy: Ulica: Nr domu: Lokal:

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

3. Powierzenie przetwarzania danych osobowych:

- * 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).

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

- * administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

- * zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
- * przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa
- * 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 - w przypadku odpowiedzi twierdzącej, należy opisać te zadania:
- * przetwarzanie jest niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

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

5. Cel przetwarzania danych w zbiorze:

Realizacja zamówień, Reklamacje, Wysyłki informacyjne i rozliczeniowe z Klientami

6. Opis kategorii osób, których dane dotyczą:

Klienci sklepu

7. Zakres przetwarzanych w zbiorze danych o osobach:

- | | |
|--|---|
| * <input checked="" type="checkbox"/> nazwiska i imiona, | * <input type="checkbox"/> Numer Identyfikacji Podatkowej, |
| * <input type="checkbox"/> imiona rodziców, | * <input type="checkbox"/> miejsce pracy, |
| * <input type="checkbox"/> data urodzenia, | * <input type="checkbox"/> zawód, |
| * <input type="checkbox"/> miejsce urodzenia, | * <input type="checkbox"/> wykształcenie, |
| * <input checked="" type="checkbox"/> adres zamieszkania lub pobytu, | * <input type="checkbox"/> seria i numer dowodu osobistego, |
| * <input type="checkbox"/> numer ewidencyjny PESEL, | * <input checked="" type="checkbox"/> numer telefonu. |

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

Adres poczty elektronicznej; Alternatywny adres wysyłki

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

- | | |
|--|---|
| * <input type="checkbox"/> pochodzenie rasowe, | * <input type="checkbox"/> przynależność partyjną, |
| * <input type="checkbox"/> pochodzenie etniczne, | * <input type="checkbox"/> przynależność związkową, |
| * <input type="checkbox"/> poglądy polityczne, | * <input type="checkbox"/> stan zdrowia, |
| * <input type="checkbox"/> przekonania religijne, | * <input type="checkbox"/> kod genetyczny, |
| * <input type="checkbox"/> przekonania filozoficzne, | * <input type="checkbox"/> nałogi, |
| * <input type="checkbox"/> przynależność wyznaniową, | * <input type="checkbox"/> życie seksualne, |

b) dotyczą:

- | | |
|--|---|
| * <input type="checkbox"/> skazań, | * <input type="checkbox"/> orzeczeń o ukaraniu, |
| * <input type="checkbox"/> mandatów karnych, | * <input type="checkbox"/> innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym |

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść 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 - w przypadku odpowiedzi twierdzącej, należy podać odniesienie do przepisu tej ustawy:
- * 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 - w przypadku odpowiedzi twierdzącej należy podać jakich:
- * 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. Dane do zbioru będą zbierane:

- * od osób, których dotyczą,
- * z innych źródeł niż osoba, której dane dotyczą.

12. Dane ze zbioru będą udostępniane:

- * 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 odbiorcy danych:

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego - należy podać nazwę państwa:

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

15. Zbiór danych osobowych jest prowadzony:

- a) * centralnie,
* w architekturze rozproszonej,
- 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),
* 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 osobowych¹⁾:

- a) * został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,
* administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,
- b) * do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych
- c) * prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
- d) * została opracowana i wdrożona polityka bezpieczeństwa,
- e) * została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
- f) inne środki, oprócz wymienionych w ppkt a - e, zastosowane w celu zabezpieczenia danych:

Środki ochrony fizycznej danych:

- ✓ Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
- ✓ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
- ✓ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez całą dobę jest nadzorowany przez służbę ochrony.
- ✓ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie

lub kasie pancernej.

- ✓ Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
- ✓ Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

- ✓ Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
- ✓ Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
- ✓ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- ✓ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.
- ✓ Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
- ✓ Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
- ✓ Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
- ✓ Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
- ✓ Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
- ✓ Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
- ✓ Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- ✓ Użyto system Firewall do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych:

- ✓ Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
- ✓ Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
- ✓ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- ✓ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.
- ✓ Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- ✓ Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
- ✓ Zastosowano kryptograficzne środki ochrony danych osobowych.
- ✓ Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
- ✓ Zastosowano 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 osobom postronnym w przetwarzane dane.
- ✓ 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.

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

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 poziomie²⁾:

- * podstawowym,
- * podwyższonym,
- * wysokim,

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 zastosować środki bezpieczeństwa na poziomie wysokim;

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

.....
(data, podpis i pieczęć wnioskodawcy)