# Sklep internetowy a rejestracja w GIODO
# FAQ

1. *Uruchamiam sklep internetowy, jeszcze nie ma klientów, ale ma przygotowaną na ich przyjęcie bazę. Czy powinien już coś zrobić względem GIODO?*

**Tak. Zbiór danych powinien zostać zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych PRZED przyjęciem pierwszych wpisów do bazy.**

2. *Wiem, że dane firm rejestrujących się w sklepie internetowym nie podlegają ochronie, a jeśli do danych firmy dojdzie imię, nazwisko, mail i prywatny telefon pracownika, który składa zamówienie?*

**Dane identyfikujące firmy lub inne osoby prawne nie podlegają ochronie danych osobowych. Tym niemniej, zgodnie z orzecznictwem europejskim, podlegają takiej ochronie dane osobowe pracowników tych firm. Nawet zestaw danych zawierających tylko imię, nazwisko i telefon pracownika podlega ochronie.**

3. *Podobno bazy danych do wystawiania faktur lub paragonów nie podlegają rejestracji w GIODO. Czy za takie dane można też uznać, wykorzystywane do wysyłki, informacje teleadresowe, które klienci pozostawiają w sklepie internetowym?*

**Dane służące do wystawiania faktur i paragonów rzeczywiście nie podlegają rejestracji, ale chodzi wyłącznie o cele fakturowania. W związku z tym, jeżeli dane służą nie tylko dla celów fakturowania (czy wystawiania paragonów), ale także do wysyłki, nie podlegają niniejszemu wyłączeniu i stosuje się do nich przepisy ogólne o obowiązku rejestracji.**

**Mimo to, nie każda sprzedaż wysyłkowa musi powodować konieczność rejestracji bazy danych (patrz odpowiedź do punktu 9).**

4. *Czy należy rozdzielać zgłoszenia do bazy danych, które są tylko wstępną rejestracją klienta (bez dokonywania jakiegokolwiek zakupu) i zgłoszenia niezbędne do sfinalizowania zamówienia?*

**Należy rozdzielać takie zgłoszenia – w przypadku dobrowolnej rejestracji w sklepie przy okazji zakupu bądź na przyszłość, dane mogą być przechowywane do czasu wycofania przez klienta zgody na ich przetwarzanie.**

**W przypadku podania danych na potrzeby jednorazowego zrealizowania transakcji, dane powinny być usunięte niezwłocznie po jej sfinalizowaniu.**

5. *Czy przy rejestracji w sklepie internetowym należy klientom przedstawić do zaakceptowania jakąś formułkę o możliwości wglądu do swoich danych lub ich usuwania?*

**Administrator danych ma OBOWIĄZEK poinformowania osoby, której dane będą przetwarzane o:**

- **adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;**
- **celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;**
- **prawie dostępu do treści swoich danych oraz ich poprawiania;**
- **dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.**

**Przykładowa klauzula informacyjna:**

**Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r. nr 101, poz. 926 ze zm.) informujemy, że:**

- **administratorem danych osobowych jest XYZ sp. z o.o. z siedzibą w Krakowie, ul. Długiej 1;**
- **dane osobowe przetwarzane będą w celu marketingu produktów i usług administratora danych i nie będą udostępniane innym odbiorcom;**
- **posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania;**
- **podanie danych osobowych jest dobrowolne.**

**Powyższa klauzula nie wymaga akceptacji przez klienta sklepu.**

**(Akceptacja jest jednak wymagana do koniecznego zazwyczaj wyrażenia przez klienta zgody na przetwarzanie danych osobowych w określonym celu. Wyrażenie zgody i obowiązek informacyjny to dwa, niezależne od siebie zagadnienia i w żadnym razie nie należy ich utożsamiać.)**

6. *Czy bazy danych wykorzystywane w różnych niesklepowych usługach internetowych podlegają ochronie, a jeśli tak, to w jakich wariantach?*

   *baza subskrybentów newslettera:*
   - *imię, mail;*
   - *imię, nazwisko, mail (plus np. wiek, płeć, miasto zamieszkania);*

   *baza forum dyskusyjnego lub portalu społecznościowego:*
   - *zdjęcie, imię, mail;*
   - *zdjęcie, imię, nazwisko, mail (plus np. wiek, płeć, telefon, adres zamieszkania);*

   *system kredytowo-pożyczkowy lub rekrutacyjny:*
   - *pełne dane osobowe, PESEL, wysokość zarobków;*
   - *pełne dane osobowe, PESEL, wysokość zarobków, stan w rejestrach (skazanych, dłużników itp. oraz np. historia zawodowa i edukacyjna).*

**Wszystkie powyższe warianty zawierają lub mogą zawierać podlegające ochronie dane osobowe – zaleca się postępowanie z nimi jak z danymi osobowymi.**

**Sam adres e-mail, zgodnie z orzecznictwem, może niekiedy zawierać dane osobowe podlegające ochronie. Należałoby więc zabezpieczyć się przed związanym z tym potencjalnym ryzykiem.**

**Wszystkie warianty zawierają dane osobowe podlegające ochronie, przy czym punkt „system kredytowo-pożyczkowy lub rekrutacyjny" zawiera dane osobowe tzw. „wrażliwe" (które wymagają szczególnej ochrony).**

7. *Jaki jest tryb zawiadomienia osób, które zarejestrowały się w bazie, o tym, że właśnie tego dokonały?*

**Zawiadomienie po zarejestrowaniu się klienta nie wchodzi w skład obowiązku informacyjnego administratora danych.**

**Jeżeli obowiązek informacyjny został zrealizowany wcześniej, treść wysyłanego potwierdzenia może być dowolna, gdyż potwierdzenie takie nie jest w ogóle wymagane z punktu widzenia ochrony danych osobowych. Jeżeli zaś obowiązek informacyjny nie został spełniony wcześniej, treść również jest dowolna z tym, że wskazane byłoby zawrzeć w niej informacje pozwalające spełnić obowiązek informacyjny (patrz punkt 5).**

8. Jaki powinien być t*ryb zawiadomienia osób znajdujących się w bazie o przekazaniu bazy innemu podmiotowi (np. sprzedaż sklepu internetowego innej firmie) albo zmianie adresu sklepu internetowego (ktoś się rejestrował w abc.pl, a nagle staje się też zarejestrowanym użytkownikiem pod xyz.pl)?*

**W przypadku przekazania bazy innemu podmiotowi, należy ponownie poinformować o:**
- **adresie siedziby i pełnej nazwie tego podmiotu, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu zamieszkania oraz imieniu i nazwisku tej osoby,**
- **celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, oraz o**
- **prawie dostępu do treści swoich danych oraz ich poprawiania.**

**Dodatkowo, należy wskazać podmiot, od którego pochodzą dane (nazwę poprzedniej firmy) oraz pouczyć osobę, której dane mają być przetwarzane o przysługujących jej tzw. uprawnieniach kontrolnych z art. 32 ust. 1 pkt 7 i 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.**

**Zawiadomienie powinno być indywidualne (nie w formie ogłoszenia).**

**Należy przy tym zauważyć, że powyższe stwierdzenia odnoszą się do sytuacji przekazania danych innemu podmiotowi, natomiast odrębny tryb stosuje się do tzw. udostępniania danych (patrz punkt 10).**

**W ustawach i w orzecznictwie brakuje wskazań dotyczących obowiązków administratora danych w sytuacji, kiedy następuje tylko zmiana adresu internetowego sklepu – np. z abc.pl na xyz.pl (lub dodanie kolejnego adresu – np. abc.com.pl). Wydaje się, że**

**skoro podmiot – administrator danych – pozostaje ten sam, wskazana wyżej procedura nie obowiązuje. Warto jednak powiadomić osoby zarejestrowane w bazie o zmianie adresu, jako że może to mieć wpływ na wykonywanie przez nich prawa dostępu do danych i do ich poprawiania.**

9. *Jak długo można przechowywać dane osobowe, a w szczególności – czy można je przechowywać „w nieskończoność”?*

**Teoretycznie „w nieskończoność” można przechowywać dane objęte zgodą na przetwarzanie wyrażoną przez osobę, której te dane dotyczą. Ograniczeniem jest jednak to, że dane mogą być przetwarzane jedynie do momentu, w którym cel ich przetwarzania zostanie zrealizowany lub przestanie istnieć.**

**Bazy danych mogą być przetwarzane do zrealizowania rzeczywistego celu przetwarzania. Cel ten stanowi zarazem podstawę prawną dokonywania czynności przetwarzania i w przypadku, gdy się zdezaktualizuje, dane osobowe powinny być usunięte lub zanonimizowane.**

**Przetwarzanie danych dla celów zrealizowania określonej transakcji, które byłyby usuwane lub anonimizowane* niezwłocznie po dokonaniu transakcji nie wymaga rejestracji w GIODO.**

*** Anonimizacja oznacza usunięcie wszelkich danych, które mogą wskazywać na konkretną osobę i pozostawienie np. tylko numeru zamówienia, nazwy towaru i ceny.**

10. *Kto może mieć dostęp do danych klientów mojego sklepu?*

**Dostęp do danych może mieć administrator danych oraz osoby upoważnione przez niego do przetwarzania danych.**

**Pomijając tzw. przekazanie danych (patrz punkt 8), dane osobowe mogą być udostępnione podmiotom zewnętrznym wyłącznie, gdy odbywa się to w ramach celu przetwarzania danych (z reguły wymagane jest wyrażenie przez klienta zgody na przetwarzanie danych w celu obejmującym ich udostępnianie).**

11. *Czy są procedury postępowania z bazami danych w sytuacjach problemowych (np. podejrzenie, że osoby niepowołane uzyskały dostęp do bazy, baza uległa częściowemu lub całkowitemu zniszczeniu, omyłkowo przekazano jednemu z klientów dane drugiego)?*

**Baza całkowicie bądź częściowo zniszczona lub zmodyfikowana w sposób nieautoryzowany, która nie daje gwarancji swojej integralności, nie może być dalej w jakikolwiek sposób przetwarzana. Wolno natomiast używać kompletnej bazy danych przywróconej z kopii zapasowej.**

**W przypadku omyłkowego przekazania danych innej osobie brak jest wytycznych dotyczących trybu postępowania administratora danych.**

**Należy liczyć się z tym, że odpowiedzialność za zabezpieczenie przed dostępem do bazy danych osób niepowołanych spoczywa na administratorze danych. W takich wypadkach administrator danych może być narażony na odpowiedzialność karną z przepisów art. 51 i 52 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Dodatkowo w grę może wchodzić cywilnoprawna odpowiedzialność odszkodowawcza administratora danych. Z kolei osobie, która nie będąc do tego uprawnioną uzyskała dostęp do bazy danych, może grozić odpowiedzialność karna z art. 267 i 268 ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553, z późn. zm.).**

12. *Jak, od strony zabezpieczeń i rozwiązań technicznych, powinny być przechowywane i przetwarzane dane osobowe?*

**Odnośnie zabezpieczeń antywłamaniowych, przeciwpożarowych, stałego numeru IP itp. – nie ma w tym zakresie obowiązków wynikających z powszechnie obowiązującego prawa. O konieczności zastosowania takich czy innych środków decyduje według swojego uznania administrator danych, który jest zobowiązany do zapewnienia bezpieczeństwa zbiorom danych osobowych.**

**Niezależnie od wielkości bazy danych (mała czy duża) i od celu przetwarzania danych osobowych (fakturowanie, funkcjonowanie portalu społecznościowego itd.), wymogi bezpieczeństwa ustalane są wg kryteriów podanych w poniższej tabeli.**

## Warunki techniczne systemu informatycznego służącego do przetwarzania danych osobowych

| | wymagany poziom bezpieczeństwa | serwer wirtualny lub dedykowany w dowolnej firmie hostingowej* | umowa powierzenia przetwarzania danych zewnętrznemu podmiotowi | UPS, antywirus, kontrola dostępu do danych (logi), regularnie tworzone kopie zapasowe | firewall | kryptograficzna ochrona uwierzytelnienia (SSL)** |
|---|---|---|---|---|---|---|
| system informatyczny, na którym przechowywane są dane osobowe nie ma dostępu do sieci publicznej (internetu) | podstawowy | możliwy | możliwa | konieczne | niekonieczny | niekonieczna |
| system jw., ale przetwarzający także „dane wrażliwe” | podwyższony | możliwy | możliwa | konieczne | niekonieczny | niekonieczna |
| system informatyczny połączony z internetem | wysoki | możliwy | możliwa | konieczne | konieczny | konieczna |

*** Zawsze jednak konieczne jest odpowiednie zabezpieczenie przed zmianami bez upoważnienia lub zniszczeniem przez hostingodawcę.**
**Każdą bazy danych osobowych można też utrzymywać na serwerze własnym, z uwzględnieniem wymogów dotyczących bezpieczeństwa.**

**** Nieważne, który z wariantów protokołu SSL będzie użyty, ponieważ każdy z nich spełnia wymóg „ochrony kryptograficznej”, a wybór jednego z nich zależy tylko od wymagań (np. ochrony transakcji) związanych z funkcjonowaniem systemu.**

* * *

Akty prawne:

- **Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926** (Ostatnia nowelizacja ustawy o ochronie danych osobowych miała miejsce w 2007 r. Większe zmiany w zasadach ochrony danych osobowych mogą nastąpić w latach 2013–2014, w związku z planowanym na jesień 2011 pracami nad nową dyrektywą europejską.)
- **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, Dz. U. z 2004 r. Nr 100, poz. 1024.**

Warto przeczytać również:

- *Ochrona danych osobowych. Komentarz*, J. Barta, R. Markiewicz, P. Fajgielski, LEX 2007;
- *Outsourcing danych osobowych w działalności przedsiębiorstw*, A. Krasuski, LexisNexis 2010;
- Informacje na stronach www.giodo.gov.pl – w zakresie przyjętej praktyki interpretacji przepisów.