# 15.

# Przetwarzanie i ochrona danych osobowych

Kwestie przetwarzania i ochrony danych osobowych reguluje **Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych ( tekst jednolity Dz. U. 2016 poz. 922 )** oraz **akty wykonawcze** do niej, tj.: **Rozporządzenia Ministra Spraw Wewnętrznych i Administracji oraz Rozporządzenia Ministra Administracji i Cyfryzacji.** Te ostatnie to akty niższego rzędu, doprecyzowujące a nie tworzące nowe reguły, to jednak w polskim systemie prawnym stanowią zazwyczaj wyznaczniki praktycznej realizacji wielu ogólnych wymagań zawartych w ustawie. W praktyce okazuje się jednak, że zasady ochrony danych osobowych reguluje ponad sto rozmaitych aktów prawnych.

**Dla większości podmiotów przetwarzających dane osobowe najistotniejsza będzie sama ustawa o ochronie danych osobowych oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych ( Dz. U. 2004 r., Nr 100, poz. 1024 ).**

Ustawa określa:

- zasady przetwarzania danych osobowych osób fizycznych
- prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych
- organy ochrony danych osobowych
- kompetencje Generalnego Inspektora Ochrony Danych Osobowych
- zasady zabezpieczania danych osobowych
- zasady rejestracji zbiorów danych osobowych
- zasady przekazywania danych osobowych do państwa trzeciego.



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

## Zakres zastosowania ustawy o ochronie danych osobowych

Ustawę stosuje się do przetwarzania danych osobowych:

- w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
- w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

W odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 ustawy.

Przykłady:

- ✓ wszelkie materiały gromadzone w formie akt, w tym sądowe, prokuratorskie, policyjne i inne zawierające dane osobowe, są zbiorem danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych.
- ✓ zbiorem, zgodnie z art. 7 pkt 1 ustawy, jest każdy posiadający strukturę, zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy też podzielony funkcjonalnie. Zbiór akt postępowania administracyjnego zawierając dane stron, ich adresy i inne informacje, spełnia te kryteria i wobec tego jest zbiorem danych w rozumieniu ustawy. Na organie administracji (gminie) ciążą zatem takie same obowiązki, jak na innych administratorach danych, w szczególności zaś obowiązek właściwego zabezpieczenia danych.

Ustawę stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych.

Ustawę stosuje się również do:

- podmiotów niepublicznych realizujących zadania publiczne,
- osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych,


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Ustawy nie stosuje się do:

- osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych[1],
- podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych.
- Ustawy, z wyjątkiem przepisów art. 14 - 19 i art. 36 ust. 1, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

## PRZEDMIOT OCHRONY (USTAWY)

Przedmiotem ustawy są **wszystkie dane dotyczące osób fizycznych.** Osoba fizyczna to określenie człowieka w prawie cywilnym – od chwili narodzenia do śmierci. W konsekwencji ustawa chroni dane osobowe jedynie osób żyjących. Warto też podkreślić, że dla stosowania ustawy nie ma znaczenia narodowość osób, których dane są przetwarzane.

[1] W tym przypadku „osobą fizyczną", nie może być żadna zbiorowość czy podmiot, tj. przedsiębiorstwo, spółka (nawet osobowa), korporacje, stowarzyszenia czy kluby, bez względu na ich wielkość. Może to być jednak grupa osób fizycznych, pozostająca w wyraźnym związku osobistym, w szczególności pokrewieństwa lub powinowactwa. Wyjmując tym samym spod restrykcji ustawowych wspólnoty rodzinne. W przypadku celów przetwarzania, determinanty są nieostre i trudno jest znaleźć granicę pomiędzy czynnościami „osobistymi lub domowymi", a tymi, które już takiego waloru nie mają, to jednak nie napotyka się tutaj na nadużycia tego wyjątku. Powszechnie przyjmuje się nawet, że takim rodzajem działalności może być nawet taka, która ma cechy czynności zarobkowych, np. działalność kolekcjonerska czy udział w aukcjach elektronicznych. Z tym podstawowym zastrzeżeniem, że osoba fizyczna nie realizuje tego w ramach prowadzonej działalności gospodarcze.

**Przykład:** *Za cel osobisty lub domowy należy uznać przechowywanie danych teleadresowych, nawet w dostępnym dla wszystkich domowników notatniku papierowym czy elektronicznym*.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

## POJĘCIE DANYCH OSOBOWYCH

Zgodnie z aktem prawnym **danymi osobowymi są „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej" (Art. 6 ust. 1 Dz. U. 2016 poz. 922).**

- 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. (Art. 6 ust. 2)
- Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. (Art. 6 ust.3)

Nie istnieje jednak żaden ustawowy katalog informacji, które można by uznać za dane osobowe. W praktyce, dowolna informacja dotycząca osoby fizycznej, może stanowić dane osobowe.

Dane osobowe należy rozumieć szeroko – od wyglądu osoby, poprzez jej imię i nazwisko, numery PESEL, kolor oczu, odciski palców, nawyki ubraniowe, aż po pozycję społeczną.

Daną osobową nie będzie pojedyncza informacja o dużym stopniu ogólności, np. nazwa ulicy, numer domu czy wysokość wynagrodzenia. Taka informacja będzie jednak stanowić daną osobową wówczas, gdy zostanie ona zestawiona z innymi dodatkowymi informacjami, które w konsekwencji będzie można odnieść do konkretnej osoby.

Informacja „zarabia 5 tys. zł miesięcznie" albo „właściciel czarnego Porsche" nic nie mówi o konkretnej osobie, ale nabierze charakteru danych osobowych, gdy zostanie połączona z danymi:

- **dotyczącymi zidentyfikowanej osoby** (np.: zarabia 5 tys. zł miesięcznie + Jan Kowalski, mieszkający przy ul. Stawki w Radomiu),
- **umożliwiającymi łatwe zidentyfikowanie osoby** (np.: właściciel czarnego Porsche + wojewoda mazowiecki). Dane, które wcześniej nie miały charakteru danych osobowych, nabrały ich po dodaniu informacji, identyfikujących osobę (imię, nazwisko i adres) lub pozwalających na identyfikację (piastowanie urzędu w określonej miejscowości lub regionie).


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

Przykład 1:

Numer PESEL dla administracji publicznej będzie stanowił daną osobową, gdyż pracownicy urzędu, mając dostęp do innych baz, są w stanie zidentyfikować osobę za pomocą tego numeru. Natomiast dla małego przedsiębiorcy, który nie ma dostępu do żadnych baz i zbiera wyłącznie numery PESEL (bez zestawiania ich z imieniem i nazwiskiem), będą to wyłącznie ciągi nic niemówiących cyfr.

Przykład 2:

Numer rejestracyjny samochodu dla przedsiębiorcy niemającego dostępu do odpowiednich baz danych nie pozwoli na identyfikację właściciela pojazdu. (Może najwyżej dać wiedzę, że właściciel auta zarejestrował pojazd w określonej miejscowości). Ale dla firmy detektywistycznej, która na podstawie numeru jest w stanie zidentyfikować właściciela za pomocą odpowiednich instrumentów, numer rejestracyjny będzie stanowić daną osobową.

RODZAJE DANYCH OSOBOWYCH

Ustawa kategoryzuje dane dzieląc je na **dane osobowe zwykłe i dane wrażliwe, zwane też sensytywnymi**.

| Dane zwykłe | Dane wrażliwe |
|---|---|
| brak wyliczenia (wszelkie inne dane osobowe oprócz danych wrażliwych) | • 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 (art. 27 ust. 1 ) |

! Warto dodać, że informacja o tym, że osoba nigdy nie była karana również stanowi dane wrażliwe. Wszystkie pozostałe informacje to dane zwykłe.

**Ważne**

**Przetwarzanie danych podlegających szczególnej ochronie (wrażliwych) co do zasady jest zabronione. Ustawa wprowadza od tego kilka wyjątków ujętych w zamknięty katalog.**



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

**Przykład:** *Przedsiębiorca w celu zapewnienia pracownikom palarni zbiera informacje, którzy pracownicy palą papierosy. Następuje proces zbierania danych osobowych wrażliwych.*

## GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Z mocy ustawy (Art. 8) nad prawidłowym stosowaniem przepisów o ochronie danych osobowych czuwa Generalny Inspektor Ochrony Danych Osobowych **(GIODO)**.

### Zadania i kompetencje Generalnego Inspektora Ochrony Danych Osobowych

Zadania i kompetencje GIODO wyznaczają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r., poz. 2135).

W świetle Art. 12 ustawy GIODO jest uprawniony do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- zapewnienia wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym, wynikających z wydanych decyzji, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji,
- prowadzenia rejestru zbiorów danych oraz rejestru administratorów bezpieczeństwa informacji, a także udzielania informacji o zarejestrowanych zbiorach danych i zarejestrowanych administratorach bezpieczeństwa informacji,
- opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenia w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

W przypadku naruszenia przepisów o ochronie danych osobowych, Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

- usunięcie uchybień,
- uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
- wstrzymanie przekazywania danych osobowych do państwa trzeciego,
- zabezpieczenie danych lub przekazanie ich innym podmiotom,
- usunięcie danych osobowych.

**W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.**

## ADMINISTRATOR DANYCH OSOBOWYCH (ADO)

Jeżeli GIODO pełni nadzór nad ochroną danych osobowych w skali makro to w mniejszej skali ustawodawca, uznając wagę danych osobowych, nakazuje pełnić nad nimi nadzór każdemu, kto je przetwarza. Każdy podmiot, przetwarzający dane osobowe zobowiązany jest nadzorować ich bezpieczeństwo. Nadzór ten pełnić ma **Administrator Danych Osobowych** – „właściciel" zebranych danych. Administratorem danych osobowych (ADO) jest organ, jednostka organizacyjna, podmiot lub osoba samodzielnie decydująca o celach i środkach przetwarzania danych osobowych. To na nim ciąży odpowiedzialność za należyte przetwarzanie danych oraz prowadzenie odpowiedniej polityki bezpieczeństwa informacji. Administratorem danych mogą być podmioty publiczne (organy państwowe, samorządu terytorialnego oraz państwowe i samorządowe jednostki organizacyjne), oraz podmioty prywatne, czyli np.:

- spółki jawne,
- spółki partnerskie,
- spółki komandytowe,
- spółki komandytowo–akcyjne,
- spółki z ograniczoną odpowiedzialnością,


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

— spółki akcyjne,

— osoby fizyczne prowadzące działalność gospodarczą,

— osoby, które nie prowadzą działalności gospodarczej[2].

Uznanie podmiotu za Administratora danych osobowych, przesądza, że musi on wypełniać określone

ustawowe obowiązki:

- **informacyjny** wypełniany przy zbieraniu danych osobowych (musi poinformować o fakcie zbierania danych osobę, której dane zbiera);
- **zachowania szczególnej staranności** przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza;
- **udzielania informacji** o zakresie przetwarzanych danych osobowych;
- **uzupełniania, uaktualnienia, sprostowania danych**, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;
- **stosowania środków technicznych** (np. szafy zamykane na klucz) i **organizacyjnych zapewniających ochronę przetwarzanych danych osobowych** (zasady wydawania kluczy do pokoi);
- **kontroli które dane, kiedy i przez kogo zostały wprowadzone do zbioru** oraz komu są one przekazywane;
- **prowadzenia ewidencji osób upoważnionych** do przetwarzania danych osobowych;
- **zgłaszania zbioru do rejestracji** Generalnemu Inspektorowi w przypadkach przewidzianych prawem

[2] Administratorem danych osobowych nie będą organy wcześniej wspomnianych podmiotów, czyli np.: zarząd i poszczególni członkowie zarządu, rada nadzorcza i członkowie rady nadzorczej, dyrektorzy departamentów, wspólnicy, partnerzy, komplementariusze.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

## ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI (ABI)

**Administrator danych osobowych może powołać Administratora bezpieczeństwa informacji (ABI) – czyli osobę nadzorującą z jego upoważnienia przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych – poprzez powierzenie zadań z zakresu ochrony danych osobowych swojemu pracownikowi**. Wybór ten wiąże się z przeszkoleniem pracownika w zakresie wymagań przepisów prawa (Ustawa o ochronie danych osobowych, przepisy sektorowe czyli np. aspekty prawa telekomunikacyjnego itd.). ale przede wszystkim z zapoznaniem go z zasadami ochrony, które będzie potrafił wprowadzać w życie. Powierzenie funkcji Administratora bezpieczeństwa informacji już zatrudnionemu pracownikowi oznacza konieczność zmiany struktury organizacyjnej – chodzi o bezpośrednią podległość Administratora bezpieczeństwa informacji pod kierownika jednostki.

**Administrator danych osobowych może powołać Administratora bezpieczeństwa informacji poprzez zawarcie umowy powierzenia danych** (outsourcing), czyli skorzystanie z usług profesjonalisty mającego doświadczenie w pełnieniu obowiązków Administratora bezpieczeństwa informacji. Jest to sytuacja najbardziej optymalna, jakkolwiek wiąże się z dodatkowymi kosztami.

**Administrator danych osobowych może nie powoływać Administratora bezpieczeństwa informacji**. Sytuacja ta występuje wtedy, kiedy administrator danych uznaje, że sam jest w stanie spełnić wszystkie obowiązki z zakresu ochrony danych osobowych. Jest to opcja, która wydaje się najtańsza. Wiąże się jednak z koniecznością samodzielnego przeszkolenia się przez podmiot w zakresie ochrony danych osobowych, wdrożenia stosownej dokumentacji, przy jednoczesnym prowadzeniu działalności statutowej.

### POWOŁANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

W ustawie wymagania stawiane Administratorowi bezpieczeństwa informacji nominalnie nie są wysokie. Administrator:

1) musi mieć pełną zdolność do wykonywania czynności prawnych (musi być pełnoletni, nie może

być ubezwłasnowolniony) oraz korzystać z pełni praw publicznych.

2) nie może być osobą karaną za przestępstwo z winy umyślnej.



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

3) ma podlegać bezpośrednio kierownikowi podmiotu np. zarządowi (art. 36a, ust. 7)

4) powinien mieć odpowiednią wiedzę z zakresu ochrony danych osobowych.

**Administrator bezpieczeństwa informacji nie ma obowiązku legitymować się wykształceniem wyższym, w szczególności wykształceniem prawniczym !**

**Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania !**

OBOWIĄZKI ABI

Z punktu widzenia wymogów ustawowych Administrator bezpieczeństwa informacji ma następujące obowiązki:

- prowadzenie rejestru zbiorów danych osobowych;
- opracowywanie dokumentacji z zakresu ochrony danych osobowych (np. Polityka Bezpieczeństwa Informacji);
- rejestracja określonych zbiorów u Generalnego Inspektora;
- nadzorowanie dokumentacji dotyczącej;
- dokonywanie sprawdzeń zgodności przetwarzania danych z przepisami;
- opracowywanie sprawozdań na podstawie dokonanych sprawdzeń.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

Zapewnienie należytego poziomu ochrony systemów informatycznych z każdym rokiem staje się coraz ważniejszym elementem polityki bezpieczeństwa informacji. Do tego stopnia, że na podmiot, który przetwarza dane osobowe w systemie informatycznym, nałożono obowiązek opracowania **Instrukcji Zarządzania Systemów Informatycznych.**

Nakłada ona na Administratora danych osobowych szereg obowiązków począwszy od czuwania nad automatycznym wylogowywaniem z systemu, jeżeli użytkownik urządzenia jest nieaktywny, poprzez utworzenie dla każdego użytkownika własnego konta, z poziomu którego może zalogować się do komputera (lub całego systemu), a skończywszy na okresowej zmianie haseł i dbaniu o ich odpowiednią siłę.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

Ponieważ Administrator bezpieczeństwa informacji nie zawsze będzie potrafił wypełnić obowiązki związane z zapewnieniem bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych, Administrator danych osobowych może powołać Administratora systemu informatycznego (ASI). Potrzeba powołania tego ostatniego wynika bardziej z praktyki niż z samych przepisów prawa. Zawsze jednak będzie to informatyk, który zajmuje się zarządzaniem systemem informatycznym i odpowiada za jego sprawne działanie.

**W hierarchii podmiotu Administrator systemów informatycznych musi podlegać Administratorowi bezpieczeństwa informacji, który może delegować na Administratora systemów informatycznych część swoich obowiązków.**

## AKTY WYKONAWCZE

Najważniejszym przepisem wykonawczym wydanym zgodnie z dyspozycją ustawy jest **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.**

Zgodnie z dyspozycją tytułu w zakresie regulacji przedmiotowego Rozporządzenia znajdują się takie obszary, jak:

1) podstawowe wymogi bezpieczeństwa dla systemów informatycznych służących do przetwarzania danych osobowych;

2) wymagania w zakresie minimalnej funkcjonalności systemów informatycznych, w szczególności w zakresie odnotowywania udostępniania danych osobowych;

3) zakres dokumentacji opisującej:

a) sposób przetwarzania danych osobowych,

b) środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych.

❖



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

# PRZETWARZANIE DANYCH OSOBOWYCH

## PRZESŁANKI PRZETWARZANIA DANYCH OSOBOWYCH ZWYKŁYCH

**Prawo określa pięć niezależnych i autonomicznych podstaw przetwarzania danych osobowych:**

1) osoba, której dane dotyczą, wyrazi na to zgodę (art. 23 ust. 1. 1. Ustawy);

2) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest stroną umowy lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (art. 23 ust. 1. 3 Ustawy);

3) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1. 2 Ustawy);

4) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (art. 23 ust. 1.4 Ustawy);

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych […], a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (art. 23 ust. 1.5). (Za prawnie usprawiedliwiony cel, uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych).

## PRZESŁANKI PRZETWARZANIA DANYCH OSOBOWYCH WRAŻLIWYCH

Należy mieć na względzie, że dane wrażliwe muszą również spełniać wymogi ogólne dla uznania ich za dane osobowe „zwykłe". W szczególności muszą dotyczyć zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przetwarzanie danych osobowych wrażliwych każdorazowo wymaga spełnienia warunków ustawowych (wymienione w art. 27 ust. 2).

1) osoba, której dane dotyczą, **wyrazi zgodę na piśmie na ich przetwarzanie**, chyba że chodzi o usunięcie dotyczących jej danych; zgoda wyrażona w sposób inny niż na piśmie jest nieskuteczna (art. 27 ust. 2, pkt 1);


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

2) **przepis szczególny innej ustawy zezwala na przetwarzanie takich danych** bez zgody osoby, której te dane dotyczą; takimi ustawami mogą być Ustawa o usługach detektywistycznych, Ustawa o zwalczaniu chorób zakaźnych (art. 27 ust. 2, pkt. 2);

3) **jest to niezbędne (…) do wykonania statutowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji,** 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 (art. 27 ust. 2, pkt. 4);

4) **przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem** (art. 27 ust. 2, pkt 5);

5) **przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób**, a zakres przetwarzanych danych jest określony w ustawie, pracodawca pragnący zebrać takie dane, powinien mieć zawsze na względzie postanowienia ustawy szczególnej (np. o związkach zawodowych, o ustawie o rozwiązaniu umowy o pracę z przyczyn nie leżących w winie pracownika, itd. (art. 27 ust. 2, pkt 6);

6) **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 (art. 27 ust. 2, pkt 7);

7) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym (art. 27 ust. 2, pkt 10).

Dziecko do ukończenia 13 roku życia nie może wyrazić zgody na przetwarzanie danych osobowych, gdyż nie ma zdolności do czynności prawnych – musi to zrobić jego rodzic. Zgodę na przetwarzanie danych wrażliwych może dać wyłącznie osoba pełnoletnia.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

## PRZETWARZANIE DANYCH OSOBOWYCH

**Pod pojęciem „przetwarzania danych", rozumie się jakiekolwiek operacje wykonywane na danych osobowych, w szczególności:**

- **zbieranie,**
- **utrwalanie,**
- **przechowywanie,**
- **opracowywanie,**
- **zmienianie,**
- **udostępnianie,**
- **usuwanie**
- **a zwłaszcza te operacje, które wykonuje się w systemach informatycznych (art. 7 ust. 2).**

**Trudno w prawie znaleźć szerszą definicję. Użycie określenia „jakiekolwiek" oznacza, że faktycznie każda czynność, jakiej zostały poddane dane osobowe, będzie oznaczać ich przetwarzanie ! (art. 7 ust 2 ustawy).**

**Przykład:** *Przedsiębiorca zakupił nowe nośniki informacji (twarde dyski). Stare nośniki zawierające dane osobowe musi zniszczyć. Niszczenie dysków twardych zawierających dane osobowe oznacza przetwarzanie danych osobowych.*

**Przykład:** *Przedsiębiorca postanowił zarchiwizować dane osobowe swoich pracowników. Oddanie dokumentów do archiwum zakładowego stanowi przetwarzanie danych osobowych.*

## UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Administrator danych osobowych przed dopuszczeniem pracownika do możliwości przetwarzania danych osobowych musi nadać mu **„Upoważnienie do przetwarzania danych osobowych**" (art. 37). Upoważnienie do przetwarzania danych osobowych nadaje się każdej osobie, która może mieć dostęp do danych osobowych, bez względu na:


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

1) rodzaj danych osobowych – „zwykłe" czy „wrażliwe";

2) sposób prowadzenia zbioru danych osobowych – kartoteka papierowa czy system informatyczny;

3) zakres dostępu do danych osobowych – zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie czy usuwanie;

4) rodzaj dostępu – jednorazowy czy stały;

5) rodzaj stosunku prawnego łączącego osobę z Administratorem danych osobowych – umowa o pracę, umowa cywilno-prawna, staż, praktyka czy wolontariat.

Najważniejszym celem nadawania „Upoważnień do przetwarzania danych osobowych" jest wypełnienie kluczowego standardu dostępu do informacji chronionych – zasady „wiedzy koniecznej" Oznacza to, że dla każdej osoby Administrator danych osobowych wyznacza indywidualny zakres dostępu do danych osobowych, dostosowany do potrzeb na zajmowanym stanowisku pracy:

1) wskazanie „zbioru danych osobowych" lub jego części;

2) szczegółowe określenie dopuszczalnych czynności na danych osobowych, tj. zbieranie, przeglądanie, aktualizowanie, kopiowanie, udostępnianie, anonimizowanie, usuwanie, itp.;

3) wyznaczenie czasu obowiązywania.

Co do zasady „Upoważnienia do przetwarzania danych osobowych" winien nadawać osobiście Administrator danych osobowych. Niemniej jednak nie istnieje przeszkoda prawna, która pozbawiała by możliwości delegowania tego uprawnienia na inną osobę. Umocowanie wybranej osoby musi jednak zostać przeprowadzone z zachowaniem wszelkich zasad nadawania pełnomocnictw, czyli:

• jednoznacznym wskazaniem osoby uprawnionej;

• precyzyjnym określeniem celu i zakresu uprawnienia;

• sporządzeniem na piśmie.

Ustawodawca nie określił wprost treści i formy, jaką ma przybrać „Upoważnienie", niemniej jednak powszechnie uznaje się, że wymagana w tym względzie jest postać pisemna. Rozwiązanie umowy z pracownikiem – bez względu na jej rodzaj – oznacza jednocześnie natychmiastową utratę uprawnień do przetwarzania danych osobowych.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

## ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI

Kluczowym elementem systemu bezpieczeństwa osobowego w procesie przetwarzania danych osobowych jest **obowiązek zachowania tajemnicy przez osoby, którym nadano „Upoważnienia do przetwarzania danych osobowych".** Ustawodawca określił tym samym odrębną „tajemnicę funkcyjną", której przedmiotem ochrony są:

• dane osobowe;

• sposoby zabezpieczenia danych osobowych (art. 39 ust. 2).

## OBOWIĄZEK INFORMACYJNY I REKTYFIKACYJNY

Na Administratora danych osobowych został nałożony specjalny **obowiązek informacyjny**. Istotnym jest, aby osoba zainteresowana (np. klient, beneficjent, pracownik) miał możliwość właściwego ocenienia sytuacji i podjęcia decyzji co do udostępnienia danych. Obowiązek informacyjny musi być wypełniony bez względu na to, w jaki sposób dane zostały zebrane, czyli: drogą pisemną, telefonicznie, w kontaktach bezpośrednich. Administrator danych osobowych jest zobowiązany poinformować osobę, której to bezpośrednio dotyczy o:

1) adresie siedziby swojego przedsiębiorstwa i jego pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców pozyskiwanych danych;

3) prawie dostępu do treści swoich danych oraz ich prawie do ich poprawiania;

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

**Wyłączenie obowiązku informacyjnego jest dozwolone wyłącznie wtedy, kiedy przepis innej ustawy na to zezwala lub osoba której dane dotyczą, wie, który podmiot przetwarza jej dane.**

Ustawa nakłada na Administratora danych osobowych również **obowiązki rektyfikacyjne**. W przypadku gdy administrator danych zbiera dane osobowe nie bezpośrednio od osoby, której dane dotyczą (np. dokonał zakupu bazy danych osobowych od innego podmiotu), jest zobowiązany 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;


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

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 prawie do ich poprawiania;

5) prawie do złożenia sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania ich innym podmiotom;

6) prawie do żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację osoby, której dane są przetwarzane.

**Wyłączenia spod obowiązku informacyjnego:**

- Przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- Dane są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego nadmiernych nakładów lub zagrażałoby realizacji celu badania,
- Dane są przetwarzane przez administratora ze sfery prawa publicznego, na podstawie przepisów prawa,
- Osoba, której dane dotyczą, posiada już informacje, które mają być jej przekazane.

OBOWIĄZEK UDZIELENIA INFORMACJI

Zgodnie z Art. 33 Ustawy na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a, a w szczególności podać w formie zrozumiałej:

1) jakie dane osobowe zawiera zbiór,

2) w jaki sposób zebrano dane,

3) w jakim celu i zakresie dane są przetwarzane,

4) w jakim zakresie oraz komu dane zostały udostępnione.

Informacji udziela się na piśmie.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

## OBOWIĄZKI SZCZEGÓLNEJ STARANNOŚCI

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

a) przetwarzane zgodnie z prawem,

b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu

niezgodnemu z tymi celami, z zastrzeżeniem ust. 2,

c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:

a) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych,

b) z zachowaniem przepisów art. 23 i 25 ustawy.

## UDOSTĘPNIANIE DANYCH OSOBOWYCH

W przypadku danych osobowych, mówiąc o udostępnieniu rozumiemy przekazywanie, oddawanie danych podmiotom, które w ustawie nazywane są **odbiorcami danych**. **W wyniku pozyskania danych odbiorcy stają się ich właścicielami – administratorami danych osobowych**. Dane możemy również udostępnić innym podmiotom w celu wykonania określonego zlecenia, mówimy wówczas o powierzeniu danych lub upoważnieniu do przetwarzania. **W rozumieniu ustawy, odbiorcą danych będzie ten: […] komu udostępnia się dane osobowe, z wyłączeniem:**

**a) osoby, której dane dotyczą,**

**b) osoby upoważnionej do przetwarzania danych,**

**c) przedstawiciela, o którym mowa w art. 31a ustawy[3],**

[3] W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

**d) podmiotu, o którym mowa w art. 31 ustawy[4],**

**e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.**

odbiorcami danych nie są:

» pracownicy upoważnieni do przetwarzania danych,

» zleceniobiorcy przetwarzający dane w ramach zlecenia,

» osoby, których dane dotyczą (mimo iż mogą te dane odbierać),

» komornik, który pozyskuje dane w postępowaniu windykacyjnym.

**Ten, kto dane osobowe kupił, jest ich odbiorcą, a następnie ich właścicielem, czyli administratorem danych osobowych !**

## POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Zlecenie innemu podmiotowi przetwarzania danych osobowych w celu realizacji określonego zadania w ustawie o ochronie danych osobowych określa się jako powierzenie przetwarzania. Zgodnie z art. 31 ust.1: Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. W Dyrektywie 95/46/WE taki podmiot określa się mianem **„procesora",** natomiast nasza ustawa nie wprowadziła krótszego terminu i **jest to po prostu „podmiot, któremu powierzono przetwarzanie danych osobowych".** Sytuacji, w których dane osobowe będą niezbędne do realizacji zlecenia może być wiele. Można z góry założyć, że zawarcia umowy powierzenia będą wymagały następujące usługi:

» prowadzenie ksiąg rachunkowych,

» przygotowanie i wysyłanie korespondencji na zlecenie (niezależnie od formy),

» prowadzenie archiwum dokumentów papierowych,

» niszczenie dokumentów,

» usługa centrum telefonicznego

» prowadzenie spraw pracowniczych (kadry),

» windykacja należności.

[4] Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

Z definicji ustawowej przetwarzania danych osobowych wynika, że przetwarzanie to operacje na danych osobowych. Jeśli celem zlecenia nie są operacje na danych, to nie należy zawierać umowy powierzenia, lecz np. umowę o zachowaniu poufności. Powierzenie jest w pewnym sensie uzupełnieniem podstaw prawnych do przetwarzania. Każdy, kto przetwarza dane osobowe, musi mieć jakąś podstawę do ich przetwarzania:

- **administrator danych osobowych musi spełniać tzw. przesłanki legalności z art. 23 ust. 1 lub art. 27 ust. 2 ustawy o ochronie danych osobowych;**
- **pracownik może przetwarzać dane osobowe na podstawie wydanego upoważnienia;**
- **zleceniobiorca przetwarza dane osobowe na podstawie umowy powierzenia.**

Ustawa wymaga, aby umowa powierzenia została zawarta na piśmie, jednak brak formy pisemnej nie oznacza jeszcze, że umowa jest nieważna, może to jednak prowadzić do sankcji w postaci decyzji administracyjnej Generalnego Inspektora Ochrony Danych Osobowych. Ustawa o ochronie danych osobowych nie nakłada żadnych ograniczeń na powierzanie danych – jeśli administrator ma prawo je przetwarzać, może również powierzyć ich przetwarzanie każdemu innemu podmiotowi. Ograniczenia mogą jednak wynikać z innych aktów prawa.

## OBOWIĄZKI ZLECENIOBIORCY

Przyjmujący dane osobowe do przetwarzania w imieniu administratora danych osobowych zobowiązany jest do spełnienia związanych z tym wymagań wynikających z ustawy. Musi je spełnić zanim zacznie przetwarzać dane, a więc zanim otrzyma je od zleceniodawcy. Wymagania te wynikają z treści art. 31 ust. 3:

**Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.**

Zleceniobiorca zobowiązany jest m.in. do:

» zabezpieczenia danych osobowych (art. 36 ust. 1),

» wydania swoim pracownikom upoważnień do przetwarzania danych osobowych (art. 37),



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

» przeszkolenia pracowników z zasad ochrony danych prowadzenia ewidencji osób upoważnionych do przetwarzania danych,

» zastosowania wymogów przewidzianych w rozporządzeniach.

Ważne

Zleceniobiorca biorąc na siebie przetwarzanie „cudzych" danych osobowych w celu realizacji umowy zobowiązuje się w zasadzie do stosowania całej ustawy o ochronie danych osobowych.

Wyjątkiem jest spełnienie przesłanek legalności, obowiązku informacyjnego i prawa do informacji oraz rejestracja i aktualizacja zbiorów danych osobowych (zbiór może zarejestrować tylko administrator danych).

## OBOWIĄZKI ZLECENIODAWCY

**Obowiązkiem zleceniodawcy, czyli administratora danych osobowych, jest zgłoszenie aktualizacji zbiorów danych osobowych i ujawnienie informacji dotyczących podmiotu, któremu powierzono przetwarzanie** (o ile powierzono do przetwarzania dane osobowe ze zbioru podlegającego rejestracji w GIODO). Wynika to z treści art. 41 ust. 1 pkt 2:

**Zgłoszenie zbioru danych do rejestracji powinno zawierać […] oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi, o którym mowa w art. 31 [...] oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania.**

W konsekwencji tego zapisu informacja o współpracujących z przedsiębiorstwem podmiotach przestaje być tajemnicą.

Ważne

Jeśli w umowie o współpracy pomiędzy podmiotami znajduje się zapis „zleceniodawca powierza zleceniobiorcy przetwarzanie danych osobowych", stanowi on jednocześnie powierzenie przetwarzania danych osobowych.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

Z obowiązku rejestracji zbioru danych zgodnie z ustawą zwolnieni są administratorzy danych:

1) objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,

[...]

2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym,

[...]

3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,

4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,

5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,

[...]

8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,

9) powszechnie dostępnych,

[...]

11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

❖



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

# KONTROLA GIODO

Generalny Inspektor Ochrony Danych Osobowych ma możliwość kontrolowania nawet tych podmiotów, które nie przetwarzają żadnych danych osobowych – choćby po to, aby się upewnić, że rzeczywiście tak jest.

Generalny Inspektor może skontrolować każdy podmiot. Oczywiste w tym świetle wydaje się, że GIODO może kontrolować też podmioty, które przetwarzają dane osobowe w imieniu przedsiębiorcy, tzw. procesorów. Wynika to zresztą bezpośrednio z art. 31 ust. 5 ustawy. Kontrola GIODO ma miejsce najczęściej wówczas, gdy do urzędu trafią sygnały o naruszaniu przez dany podmiot przepisów ustawy o ochronie danych osobowych. Najczęstszymi sygnałami są skargi poszczególnych osób. Warto przy tym zwrócić uwagę, że złożenie skargi do GIODO wiąże się z koniecznością wniesienia stosownej opłaty, więc bardzo prawdopodobne, że najpierw taka skarga zostanie skierowana do podmiotu naruszającego ustawę, a dopiero w dalszej kolejności – gdy nie przyniesie to oczekiwanego efektu – do GIODO. Generalny Inspektor podkreśla, że skupia się przede wszystkim na kontrolowaniu podmiotów, na które wpływają skargi, bo jest to sygnał, że może w nich dochodzić do poważnego naruszania przepisów. Wynika z tego, że dbając o rzetelne podejście do skarg i reklamacji klientów w zakresie przetwarzania danych osobowych, przedsiębiorcy mogą skutecznie zmniejszyć ryzyko wpłynięcia na nich skarg i, w konsekwencji, kontroli GIODO.

Niezależnie od wpływających skarg, każdego roku GIODO wybiera różne branże lub sektory działalności, którym chce się lepiej przyjrzeć. Bodźce inicjujące kontrolę mogą pochodzić od podmiotów, z którymi GIODO podpisał stosowne porozumienia. Przykładowo, w 2012 r. zostało podpisane porozumienie z Państwową Inspekcją Pracy (PIP), która zobowiązała się m.in. do zawiadamiania GIODO o stwierdzonych, w czasie swoich kontroli, nieprawidłowościach w zakresie zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Rok wcześniej zawarto porozumienie z Najwyższą Izbą Kontroli (NIK), na mocy którego strony zobowiązały się do wzajemnego przekazywania sobie informacji o nieprawidłowościach, które mogą stanowić przedmiot ich zainteresowania .

<u>Kontrole, jakie mogą wystąpić to:</u>

» kontrola z urzędu (własna inicjatywa GIODO, rozpatrywanie zgłoszeń rejestracyjnych zbiorów, skargi poszczególnych osób),

» kontrola sprawdzająca (jeśli GIODO nakazał wcześniej usunięcie uchybień),


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

» kontrola na wniosek (np. prokuratury, Państwowej Inspekcji Pracy, osoby pokrzywdzonej).

Kontrole mogą różnić się zakresem:

» kontrola kompleksowa – dotyczy wszystkich zbiorów danych osobowych i wszystkich wymogów ustawy o ochronie danych osobowych,

» kontrola częściowa – dotyczy określonych zagadnień, np. wybranego obszaru funkcjonowania organizacji lub, w opcji bardziej zawężonej, np. sprawdzenia legalności pozyskiwania danych czy sposobu realizacji obowiązku informacyjnego wobec osób, których dane są przetwarzane.

Jeśli chodzi o formę, można wyróżnić dwa rodzaje kontroli:

» kontrola na miejscu – tradycyjna forma kontroli,

» kontrola korespondencyjna („zdalna") – udzielanie pisemnych wyjaśnień GIODO.

Zazwyczaj podmiot kontrolowany informowany jest o planowanej kontroli z pewnym wyprzedzeniem telefonicznie. Następnie na piśmie (czasem faksem) przedstawiany jest przedmiot kontroli, potwierdzenie terminu i prośba o przygotowanie określonych materiałów. Nie ma obowiązku odpisywani na zawiadomienie o kontroli. Wyjątkiem jest sytuacja, gdy kontrolowanemu podmiotowi, z uzasadnionych przyczyn, nie odpowiada ustalony przez GIODO termin. Można wówczas wnioskować o jego zmianę. Przygotowując się do kontroli, należy przede wszystkim zacząć od przeanalizowania zagadnień z art. 49 – 54 ustawy o ochronie danych osobowych, których niedopełnienie grozi postępowaniem karnym. W pierwszej kolejności należy zadbać m.in. o posiadanie prawa do przetwarzania danych, właściwe zabezpieczenie danych (tak, aby osoby nieupoważnione nie miały do nich dostępu), rejestrację zbiorów oraz dopełnianie obowiązków informacyjnych względem osób, których dane są przetwarzane. Wszystkie pozostałe wymagania można uznać za mniej groźne, bo konsekwencją ich nierealizowania jest postępowanie administracyjne, mniej dotkliwe od karnego.

W czasie kontroli inspektorzy GIODO zobowiązani są posiadać stosowne upoważnienie – imienne, terminowe (ważne na okres danej kontroli) i dotyczące kontroli w konkretnym przedsiębiorstwie Prawa kontrolerów są bardzo szerokie. Mają oni m.in.prawo wstępu do pomieszczeń firmy, mogą żądać udzielenia wyjaśnień, a także uzyskiwać dostęp do wszelkich danych, mających związek z kontrolą i przeprowadzania oględzin (art. 14 ustawy).

Podstawowym obowiązkiem przedsiębiorcy jest umożliwienie przeprowadzenia kontroli. Nie można jej utrudniać ani uniemożliwiać, bo to jest karane z art. 54a ustawy.


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

Należy umożliwić inspektorom przeprowadzenie kontroli, tj.:

» składać niezbędne wyjaśnienia pisemne albo ustne,

» udostępnić żądane dokumenty do wglądu albo ich kopie,

» pozwolić na dokonanie oględzin systemów informatycznych, urządzeń i nośników służących do przetwarzania danych osobowych,

» umożliwić wgląd w dane osobowe.

Kontrola kończy się sporządzeniem protokołu (art.16 ust.1 ustawy), przy czym kontrolowany może wnieść do protokołu umotywowane zastrzeżenia i uwagi. Jeśli w trakcie kontroli stwierdzono nieprawidłowości, zgodnie z art. 61 § 4 Kodeksu postępowania administracyjnego, następuje wszczęcie postępowania administracyjnego. Kontrolowany zostaje o tym poinformowany pisemnie, otrzymuje również opis uchybień stwierdzonych w trakcie kontroli. W wyniku postępowania wydawana jest decyzja administracyjna, która może nakazać „przywrócenie stanu zgodnego z prawem" (usunięcie niezgodności z ustawą) lub umorzyć (zamknąć) postępowanie.

Jak wynika z przepisów prawa, czynności kontrolne są dla ustawodawcy niezwykle ważne. Art. 15 ust. 1 ustawy o ochronie danych osobowych nakazuje podmiotowi umożliwienie przeprowadzenia kontroli. Utrudnianie lub uniemożliwienie przeprowadzenia kontroli od 2012 r. jest karane nowymi przepisami karnymi. Udaremnianie i utrudnianie kontroli oznacza, odpowiednio, całkowite uniemożliwienie wykonania kontroli oraz doprowadzenie do tego, że kontrola napotka na przeszkody, uniemożliwiające jej osiągnięcie celu. Przykładem takiego działania może być zlecenie służbom ochrony niewpuszczenia inspektorów GIODO na teren przedsiębiorstwa. Utrudnianiem kontroli będzie też odmówienie udzielenia wyjaśnień czy niedopuszczenie do oględzin urządzeń, nośników danych, itp. Jeśli kontrolowany doprowadzi do udaremnienia albo utrudnienia kontroli niechcący, nie mając takiego zamiaru, nie będzie wówczas odpowiadał z art. 54a.

Nowością od 1 stycznia 2015 r. jest możliwość żądania przez GIODO dokonanie przez administratora bezpieczeństwa informacji „sprawdzenia" na ile organizacja zapewnia zgodność z przepisami dotyczącymi ochrony danych osobowych (art. 19b ust.1). Po jego dokonaniu należy przygotować sprawozdanie i przesłać je do GIODO.

Jeśli po kontroli, w ramach postępowania administracyjnego, Generalny Inspektor Danych Osobowych nakaże przywrócić stan zgodny z prawem, a kontrolowany się nie zastosuje do tego nakazu, GIODO ma prawo podjąć działania egzekucyjne –wystawia tytuł wykonawczy i


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

kieruje do właściwego organu wniosek o wszczęcie postępowania egzekucyjnego. Środki egzekucyjne, jakie mogą zostać zastosowane, to:

» **grzywna,**

» **wykonanie zastępcze,**

» **przymus bezpośredni**.

Grzywna jest karą najprostszą do zastosowania. Organ egzekucyjny wystawia postanowienie o zastosowaniu grzywny, a gdy nie zostanie ona uiszczona, kieruje tytuł wykonawczy do właściwego urzędu skarbowego, w wyniku czego zasądzona kwota zostanie zajęta z rachunku bankowego ukaranego. W przypadku osoby fizycznej maksymalna wysokość grzywny wynosi 10 tys. zł, w przypadku osób prawnych i jednostek organizacyjnych, nieposiadających osobowości prawnej (spółki z o.o., spółki akcyjne) – 50 tys. zł. Grzywny można nakładać wielokrotnie. W jednym postępowaniu egzekucyjnym ich łączna kwota wynosi do 50 tys. zł w przypadku osób fizycznych i do 200 tys. zł w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej.

## ODPOWIEDZIALNOŚĆ KARNA, ADMINISTRACYJNA I CYWILNA

W przypadku naruszenia ustawy o ochronie danych osobowych należy się liczyć z odpowiedzialnością administracyjną, cywilną i karną. Postępowanie administracyjne to wszystkie działania, jakie wobec administrującego danymi podejmować będzie bezpośrednio Generalny Inspektor Ochrony Danych Osobowych. Postępowanie cywilne będzie mieć miejsce, gdy w wyniku niedopełnienia obowiązków ustawowych zostaną poszkodowane osoby, których dane przetwarzano – poszkodowani mogą wówczas dochodzić swoich praw na drodze postępowania cywilnoprawnego. Postępowanie karne wynika z opisanych powyżej zapisów ustawy o ochronie danych osobowych – warto więc je znać i stosować w praktyce.

❖


LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

W odniesieniu do **ustawy o wspieraniu rodziny i systemie pieczy zastępczej (Dz. U. z dn. 10 marca 2015 r. poz. 332) stosowanie przepisów o ochronie danych osobowych reguluje artykuł 7:**

1. Podmioty i osoby realizujące zadania w zakresie wspierania rodziny i systemu pieczy zastępczej mogą przetwarzać dane osobowe osób, do których stosuje się niniejszą ustawę, oraz członków ich rodzin w zakresie niezbędnym do realizacji zadań wynikających z niniejszej ustawy.

2. Zbieranie danych, o których mowa w ust. 1, w celu realizacji zadań z zakresu wspierania rodziny i systemu pieczy zastępczej przez podmioty i osoby realizujące te zadania, nie powoduje po ich stronie obowiązku, o którym mowa w **art. 25** *zbieranie danych nie od osoby której dane dotyczą* ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922).

3. Podmioty i osoby realizujące zadania w zakresie wspierania rodziny i systemu pieczy zastępczej są obowiązane do zachowania w tajemnicy informacji o osobach, do których stosuje się niniejszą ustawę, oraz członkach ich rodzin, w tym informacji o udzielonej tym osobom pomocy i świadczeniach.

**Zasady bezpiecznego przetwarzania danych osobowych w instytucjach wspierania rodziny i pieczy zastępczej, najczęściej są opracowywane w odrębnych dokumentach w postaci tzw. polityki prowadzonej w danej placówce bądź instrukcji**.

**Przykład:**

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W POWIATOWYM CENTRUM POMOCY RODZINIE W ZGIERZU

(Patrz załącznik nr 1)



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie

Bibliografia:

Akty Normatywne:

Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych ( tekst jednolity Dz. U. 2016 poz. 922 ),

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych raz 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),

Ustawa o wspieraniu rodziny i systemie pieczy zastępczej (Dz. U. z dn. 10 marca 2015 r. poz. 332)

Pozycje zwarte:

Kępa L., *Jak w praktyce i zgodnie z prawem przetwarzać dane osobowe*, Warszawa 2015.

Kister Ł. Mendyk B., *Ochrona danych osobowych w przedsiębiorstwie – poradnik dla Małych i Średnich Przedsiębiorstw,* Warszawa 2015.



LIDER PROJEKTU
Województwo Podkarpackie - Regionalny Ośrodek Polityki Społecznej w Rzeszowie
ul. Hetmańska 120, 35-078 Rzeszów tel. 17 747 06 00 fax. 17 747 06 01 e-mail: sekretariat@rops.rzeszow.pl www.rops.rzeszow.pl
PARTNERZY PROJEKTU
Województwo Podkarpackie | Województwo Lubelskie | Województwo Podlaskie | Województwo Świętokrzyskie