

Ochrona danych osobowych w oświacie z punktu widzenia samorządu jako organu prowadzącego

Radosław Wiktorski



Kluczowe informacje o przepisach w zakresie ochrony danych osobowych



Przepisy prawa dotyczące ochrony danych osobowych

- ➔ Konstytucja RP
- ➔ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dziennik Urzędowy Wspólnot Europejskich L 281/31
- ➔ Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.)
- ➔ Rozporządzenie 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)



Przepisy prawa dotyczące ochrony danych osobowych

- ➔ Rozporządzenie z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536),
- ➔ Rozporządzenie z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. nr 94, poz. 923),
- ➔ inne akty prawne, mniej istotne w kontekście niniejszego szkolenia.



Konstytucja RP

Art. 47.

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 51.

1. Nikt nie może być obowiązany **inaczej niż na podstawie ustawy** do ujawniania informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać **innych** informacji o obywatelach **niż niezbędne** w demokratycznym państwie prawnym.

3. **Każdy ma prawo dostępu** do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

4. Każdy ma prawo do żądania **sprostowania** oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

5. Zasady i tryb gromadzenia oraz udostępniania informacji **określa ustawa**.



Kogo dotyczy?

Art. 3.

Ustawę stosuje się do:

- organów państwowych,
- **organów samorządu terytorialnego**
- **państwowych i komunalnych jednostek organizacyjnych.**

2. Ustawę stosuje się również do:

- 1) podmiotów niepublicznych realizujących zadania publiczne,
- 2) 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**



Podstawowe pojęcia

- ➔ Administrator danych
- ➔ Zbiór danych
- ➔ Dane osobowe
- ➔ Przetwarzanie danych
- ➔ Zgoda



Administrator danych

Art. 7

Ilekoć w ustawie jest mowa o:
(...)

4) administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 [zakres stosowania ustawy], **decydujące o celach i środkach** przetwarzania danych osobowych,



Zbiór danych

Art. 7

Ilekoć w ustawie jest mowa o:

1) zbiorze danych - 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,



Zbiór danych

- ➔ W sytuacji niejednoznacznej (z którą mamy do czynienia w oświacie) rozważenia wymaga sposób zdefiniowania zbiorów danych.
- ➔ Zbytne zwiększenie liczby zbiorów utrudnia zarządzanie nimi (zwłaszcza od strony formalnej)



Dane osobowe

Art. 6. u.o.d.o.

1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące **zidentyfikowanej lub możliwej do zidentyfikowania** osoby fizycznej.



Dane osobowe

Art. 6. u.o.d.o.

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.



Dane osobowe

Art. 6. u.o.d.o.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to **nadmiernych kosztów, czasu lub działań.**



Dane osobowe

Z dokumentów GIODO:

*Przykładem pojedynczej informacji stanowiącej dane osobowe jest numer PESEL. (...) Numer ten, występując nawet **bez zestawienia z innymi informacjami** o osobie, **stanowi dane osobowe**, a ich przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie o ochronie danych osobowych.*



Dane osobowe

Z dokumentów GIODO:

Adres poczty elektronicznej – bez dodatkowych informacji, umożliwiających ustalenie tożsamości osoby – zasadniczo nie stanowi danych osobowych. Występujący samodzielnie adres poczty elektronicznej można w wyjątkowych przypadkach uznać za dane osobowe, ale tylko wtedy, gdy elementy jego treści pozwalają, bez nadmiernych kosztów, czasu lub działań – na ustalenie na ich podstawie tożsamości danej osoby. Dzieje się tak w sytuacji, gdy elementami treści adresu są np. imię i nazwisko jego właściciela.



Przetwarzanie danych

Art. 7

Ilekoć w ustawie jest mowa o:
(...)

2) przetwarzaniu danych - rozumie się przez to **jakiegokolwiek** operacje wykonywane na danych osobowych, takie jak:

- zbieranie,
- utrwalanie,
- **przechowywanie**,
- opracowywanie,
- zmienianie,
- udostępnianie,
- usuwanie,

zwłaszcza te, które wykonuje się w systemach informatycznych,



Zgoda

Art. 7

Ilekcroć w ustawie jest mowa o:

(...)

5) zgodzie osoby, której dane dotyczą - rozumie się przez 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

- ➔ Z treści zgody musi w sposób niebudzący wątpliwości wynikać cel i zakres przetwarzania danych oraz kto dane będzie przetwarzał.
- ➔ Zgoda na przetwarzanie danych „zwykłych” nie musi być wyrażona na piśmie, jednak dla ewentualnych celów dowodowych zaleca się, by jeśli to możliwe była pisemna.
- ➔ Zgodna na przetwarzanie danych „wrażliwych” musi być wyrażona na piśmie.



Zasady przetwarzania danych osobowych

Ustawa jest skonstruowana wedle zasady „co nie jest dozwolone, jest zabronione”

Art. 23. 1. ustawy:

Przetwarzanie danych jest dopuszczalne
tylko wtedy, gdy:...



Art. 23.

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

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

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z **przepisu prawa**,

3) 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,

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla **dobra publicznego**,

5) 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.



Dopuszczalność przetwarzania

Pod kątem podstawy przetwarzania należy rozpatrywać **każdy konkretny zakres danych**.

Podstawę przetwarzania należy rozpatrywać zawsze w związku z **celem przetwarzania**.



Dopuszczalność przetwarzania

- ➔ Administrator danych musi umieć **wykazać** się podstawą prawną przetwarzania danych (ciężar dowodu).
- ➔ Dane **jednej** osoby mogą być przetwarzane na **różnych** podstawach prawnych.
- ➔ Podstawę przetwarzania należy odnosić do celu przetwarzania – przetwarzanie danych w **różnych celach** może mieć **różne podstawy** prawne.



Szczególna staranność

Art. 26.

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:

- 1) przetwarzane zgodnie z prawem,
- 2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2



Szczególna staranność

- 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.



Szczególna staranność

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:

- 1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych,
- 2) z zachowaniem przepisów art. 23 i 25 [dopuszczalność przetwarzania i obowiązek informacyjny].



Zasady (zbiorczo)

- ➔ **Legalności** – podstawa prawna (art. 23 lub 27),
- ➔ **Celowości** – przetwarzanie tylko w określonym, legalnym celu,
- ➔ **Czasowości** – przetwarzanie tylko do momentu osiągnięcia celu,
- ➔ **Adekwatności** – przetwarzania tylko takiego zakresu danych, który jest niezbędny dla osiągnięcia celu,
- ➔ **Merytorycznej poprawności.**



Powierzenie przetwarzania

Art. 31.

1. Administrator danych **może powierzyć** innemu podmiotowi, w drodze umowy zawartej **na piśmie**, przetwarzanie danych.
2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane **wyłącznie w zakresie i celu** przewidzianym w umowie.



Powierzenie przetwarzania

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.**



Powierzenie przetwarzania

4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy **spoczywa na administratorze danych**, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.



Zabezpieczenie danych

Art. 36.

1. Administrator danych jest obowiązany zastosować środki **techniczne i organizacyjne** zapewniające ochronę przetwarzanych danych osobowych **odpowiednią do zagrożeń oraz kategorii danych** objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, **przetwarzaniem z naruszeniem ustawy** oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.



Zabezpieczenie danych

2. Administrator danych **prowadzi dokumentację** opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

3. Administrator danych **wyznacza administratora bezpieczeństwa informacji**, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, **chyba że sam wykonuje te czynności.**



Upoważnienia do przetwarzania danych osobowych

Art. 37. Do przetwarzania danych mogą być dopuszczone **wyłącznie osoby posiadające** upoważnienie nadane przez administratora danych.

Jeżeli dane są przetwarzane przez osoby nie posiadające stosownego upoważnienia, oznacza to, że są przetwarzane z naruszeniem ustawy (dostęp osób nieuprawnionych).



Ewidencja upoważnionych

Art. 39.

1. 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.

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



Zgłoszenie zbioru do rejestracji

Art. 40.

Administrator danych jest **obowiązany zgłosić** zbiór danych do rejestracji Generalnemu Inspektorowi, **z wyjątkiem przypadków**, o których mowa w art. 43 ust. 1.



Dokumentacja

§ 3.

1. Na dokumentację, o której mowa w § 1 pkt 1, składa się **polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych, zwana dalej „instrukcją”.
2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w **formie pisemnej**.
3. Dokumentację, o której mowa w § 1 pkt 1, **wdraża administrator danych**.



Dziękuję za uwagę!

Radosław Wiktorski
radoslaw.wiktorski@vulcan.pl