



## Ochrona danych osobowych w Unii Europejskiej

Ochrona danych osobowych jest jednym z najważniejszych praw człowieka. Unia Europejska podkreśla znaczenie utrzymania równowagi między podnoszeniem poziomu bezpieczeństwa i zagwarantowaniem przestrzegania praw człowieka, w tym ochrony danych i prywatności. Wprowadzane zmiany w przepisach w zakresie ochrony danych wzmocnią prawa obywateli. Reforma ma zapewnić większą kontrolę nad danymi, dzięki czemu prywatność w epoce cyfrowej będzie nadal przestrzegana.

### Dane osobowe

W prawie unijnym „dane osobowe” definiuje się jako informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, czyli informacje o osobie, której tożsamość jest oczywista bądź przynajmniej może zostać ustalona przez uzyskanie dodatkowych informacji. Jeżeli dane dotyczące takiej osoby są przetwarzane, osoba ta jest nazywana „osobą, której dane dotyczą”.

**Czym są dane osobowe?**

- Imię i nazwisko
- Adres
- Lokalizacja
- Identyfikator internetowy
- Informacje dotyczące stanu zdrowia
- Dochody
- Profit kulturowy
- Inne

**GROMADZISZ  
PRZECHOWUJESZ  
WYKORZYSTUJESZ  
DANE?**

Musisz postępować zgodnie z przepisami.

**Przetwarzasz dane dla innych firm?**  
Dotyczy to również Ciebie.



Źródło: Komisja Europejska



Istnieją różne kategorie danych, w tym m.in. tzw. dane szczególnie chronione (wymienione w konwencji nr 108 i dyrektywie o ochronie danych), które wymagają zwiększonej ochrony i podlegają z tego powodu specjalnemu reżimowi prawnemu.

### **Podstawa prawna**

Ochrona danych osobowych obowiązuje na podstawie art. 16. Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz artykułów 7 i 8 Karty Praw Podstawowych UE. Unia Europejska dba o to, by podstawowe prawo do ochrony danych, które jest przewidziane w Karcie praw podstawowych, było przestrzegane. Art. 16 TFUE stanowi, że Parlament i Rada określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy, biura i agencje Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres stosowania prawa Unii.

Przed wejściem w życie Traktatu z Lizbony prawodawstwo unijne dotyczące ochrony danych było podzielone pomiędzy pierwszy filar (ochrona danych do celów prywatnych i handlowych) a trzeci filar (ochrona danych do celów egzekwowania prawa – na poziomie międzyrządowym). Wejście w życie Traktatu z Lizbony, na podstawie którego przestała obowiązywać struktura filarowa stało się podstawą do rozwoju bardziej skutecznego systemu ochrony danych.

W grudniu 2009 roku Rada Europejska zatwierdziła program sztokholmski na lata 2010-2014- dotyczący przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Natomiast w konkluzjach ze szczytu Rady Europejskiej w czerwcu 2014 roku określone zostały strategiczne wytyczne planowania ustawodawczego i operacyjnego na kolejne lata, zgodnie z art. 68 TFUE. Za jeden z głównych celów uznano lepszą ochronę danych osobowych w Unii Europejskiej.

### **Najważniejsze międzynarodowe instrumenty prawne w zakresie ochrony danych**

- **Karta praw podstawowych UE**

Zgodnie z art. 7 i 8 Karty praw podstawowych UE poszanowanie życia prywatnego oraz ochrona danych osobowych są ze sobą powiązane, jednak stanowią odrębne prawa podstawowe. Karta jest prawnie wiążąca dla instytucji i organów Unii Europejskiej, a także dla państw członkowskich podczas wprowadzania w życie prawa UE. Została ona bowiem włączona do Traktatu z Lizbony.

- **Konwencja 108 z 1981 r.**

Konwencja 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób jest pierwszym prawnie wiążącym instrumentem międzynarodowym przyjętym w dziedzinie ochrony



danych. Jej celem jest „zagwarantowanie [...] każdej osobie fizycznej [...] poszanowania jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych”.

- **Europejska konwencja praw człowieka (EKPC)**

W Europejskiej konwencji o ochronie praw człowieka (art.8) z 4 listopada 1950 roku znajduje się zapis o prawie do poszanowania życia prywatnego i rodzinnego: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji”

### **Instrumenty prawne UE w zakresie ochrony danych**

Na skutek dawnej struktury filarowej obowiązują obecnie różne instrumenty prawne. Obejmują one takie instrumenty w ramach dawnego pierwszego filaru:

- dyrektywa 95/46/WE o ochronie danych,
- dyrektywa 2002/58/WE w sprawie e-prywatności (zmieniona w 2009 r.),
- dyrektywa 2006/24/WE w sprawie zatrzymywania danych,
- rozporządzenie (WE) nr 45/2001 w sprawie przetwarzania danych osobowych przez instytucje i organy wspólnotowe
- w ramach dawnego trzeciego filaru:
- ramowa decyzja Rady z listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Wkrótce mają wejść w życie nowe kompleksowe ramy prawne w zakresie ochrony

- **Dyrektywa w sprawie ochrony danych (95/46/WE) – ma zostać uchylona w maju 2018 r.**

Dyrektywa 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych to centralna część prawodawstwa o ochronie danych osobowych w UE. W dyrektywie określono zasady ogólne legalności przetwarzania danych osobowych oraz ustalono prawa osób, których dane dotyczą, przewidując jednocześnie istnienie krajowych niezależnych organów nadzorczych. Dyrektywa przewiduje, że informacje osobowe mogą być przetwarzane jedynie za wyraźną zgodą osoby, której te dane dotyczą, oraz pod warunkiem uprzedniego poinformowania zainteresowanej osoby o przetwarzaniu danych.



- **Ramowa Rady 2008/977/WSiSW – ma zostać uchylona w maju 2018 r.**

Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. dotyczy ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach. Jest to sektor nieobjęty dyrektywą 95/46/WE, która odnosi się do przetwarzania danych osobowych w dawnym pierwszym filarze. Decyzja ramowa obejmuje jedynie wymianę danych policyjnych i sądowych między państwami członkowskimi, organami UE i powiązаныmi systemami, a nie obejmuje krajowego przetwarzania danych.

### **Reforma ochrony danych w UE**

W maju 2018 roku zacznie obowiązywać reforma ochrony danych w UE. W dniu 25 stycznia 2012 r. Komisja opublikowała obszerny pakiet ustawodawczy mający na celu zreformowanie przepisów UE dotyczących ochrony danych. Celem reformy jest zapewnienie ochrony danych osobowych w UE, przy jednoczesnym zwiększeniu przysługującej użytkownikom kontroli ich własnych danych i zredukowaniu kosztów ponoszonych przez przedsiębiorstwa.

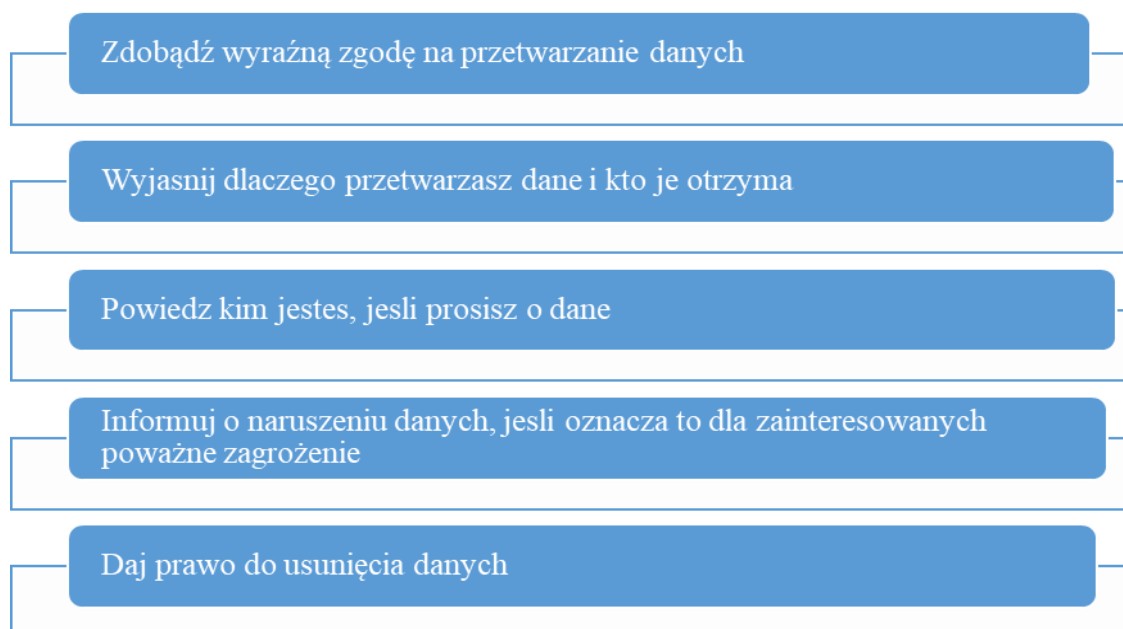
Zmiany wynikają z postępu technologicznego i postępu globalizacji, które znacząco zmieniły sposób gromadzenia naszych danych, jak i uzyskiwania do nich dostępu i wykorzystywania ich. Ponadto należy zaznaczyć, że przepisy z 1995 r. zostały w niejednakowy sposób wdrożone przez 28 państw członkowskich. Dzięki przyjęciu jednego aktu prawnego zniesiona zostanie obecna fragmentacja i kosztowne obciążenia administracyjne. Wprowadzenie zmian pomoże wzmocnić zaufanie konsumentów do usług online, co doprowadzi do wzrostu zatrudnienia i innowacji w UE.

Nowe zasady ochrony danych zostały ustalone w grudniu 2015 roku, a opublikowane w kwietniu 2016 roku. Zaczną one obowiązywać począwszy od maja 2018 roku. Nowe zasady zostały uregulowane w następujących dokumentach:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW.

## Ochrona danych osobowych w ramach prowadzenia firmy

Prowadząc działalność gospodarczą należy pamiętać o tym, by chronić prawa osób przekazujących nam swoje dane. Zasadę ochrony danych należy stosować już w fazie projektowania. Poniżej przedstawiono zasady, które warto stosować w firmie w celu ochrony danych osobowych.



Prowadząc firmę trzeba z należyta starannością podchodzić do kwestii ochrony danych osobowych. Nieprzestrzeganie zasad ochrony danych osobowych może prowadzić do kar finansowych.

## Koszty nieprzestrzegania przepisów



Twój miejscowy organ ochrony danych kontroluje przestrzeganie przepisów, jego działania są koordynowane na szczeblu unijnym. Omijanie prawa może dużo kosztować.



Zgodnie z nowymi przepisami w niektórych sytuacjach konieczne będzie powołanie inspektora ochrony danych.

### Ustal, czy potrzebujesz inspektora ochrony danych

Nie zawsze jest to obowiązkowe. Jest to uzależnione od rodzaju i ilości gromadzonych danych, od tego czy ich przetwarzanie jest podstawą Twojej działalności i czy robisz to na dużą skalę.

Przetwarzasz dane osobowe na potrzeby ukierunkowania reklam za pośrednictwem wyszukiwarek internetowych w oparciu o zachowanie użytkowników w środowisku on-line.	Tak 
Raz w roku wysyłasz klientom reklamę promującą Twoją działającą lokalnie firmę sektora spożywczego.	Nie
Jesteś lekarzem pierwszego kontaktu i gromadysz dane dotyczące zdrowia pacjentów.	Nie
Przetwarzasz dane osobowe dotyczące genetyki i zdrowia dla szpitala.	Tak 

Zródło: Komisja Europejska

## Europejski Inspektor Ochrony Danych (EIOD)



Europejski Inspektor Ochrony Danych (EIOD) to niezależny organ nadzorczy gwarantujący, że instytucje oraz organy UE przestrzegają swych zobowiązań w dziedzinie ochrony danych.

Podstawowymi obowiązkami EIOD są:

- nadzór,
- konsultacja
- współpraca.

Funkcję Europejskiego Inspektora Ochrony Danych sprawuje obecnie Giovanni Buttarelli, a jego zastępcą jest Wojciech Wiewiórski. **Inspektor** i jego **zastępca** są mianowani na odnawialną pięcioletnią kadencję. Za wykonywanie bieżących zadań odpowiadają **dwie jednostki organizacyjne**:

- Dział Nadzoru i Egzekwowania Prawa - **ocenia przestrzeganie przepisów o ochronie danych** przez instytucje i organy UE,
- Dział Polityki i Konsultacji - doradza unijnym prawodawcom w różnych obszarach polityki i w sprawie projektów nowych aktów prawnych.





## Zadania Europejskiego Inspektora Ochrony Danych

Kontrola instytucji UE w zakresie ochrony danych

Doradztwo instytucjom UE w kwestiach związanych z ochroną danych

Zajmowanie się skargami i prowadzenie dochodzeń

Współpraca z krajowymi organami w państwach UE

Monitoring nowych technologii pod względem ochrony danych

Organem, który zajmuje się ochroną danych osobowych jest także grupa robocza - niezależny organ doradczy w sprawie ochrony danych i prywatności powołany na mocy art. 29 dyrektywy w sprawie ochrony danych. Grupa składa się z przedstawicieli krajowych organów ochrony danych państw członkowskich UE, Europejskiego Inspektora Ochrony Danych oraz Komisji Europejskiej. Wydaje ona zalecenia, opinie i dokumenty robocze. Powołana zgodnie z art. 29 grupa robocza zostanie zastąpiona Europejską Radą Ochrony Danych na mocy ogólnego rozporządzenia o ochronie danych.

### Co zrobić, gdy instytucje lub organy UE ujawniają nasze dane osobowe?

Instytucjom i organom UE nie wolno przetwarzać danych osobowych ujawniających:

- **pochodzenie rasowe lub etniczne,**
- **poglądy polityczne,**
- **poglądy religijne lub filozoficzne,**
- **przynależność do związków zawodowych.**

Zakazane jest także przetwarzanie danych dotyczących **sytuacji zdrowotnej** lub **orientacji seksualnej**, o ile nie jest to niezbędne dla celów medycznych. Jednak nawet wówczas dane powinny być przeprowadzane przez pracownika służby zdrowia lub inną osobę związaną przysięgą do zachowania tajemnicy zawodowej.

Każdy, kto uzna, że jego **prawa do poszanowania prywatności** zostały naruszone przez instytucję lub organ UE, w **pierwszej kolejności powinien poinformować urzędnika UE odpowiedzialnego za przetwarzanie danych**. Jeśli nie przyniesie to rezultatu, należy



skontaktować się z właściwym inspektorem ochrony danych w instytucji lub organie, gdzie doszło do naruszenia danych.

Jeśli w dalszym ciągu wynik jest niezadowolający, można **złożyć skargę** do Europejskiego Inspektora Ochrony Danych za pomocą formularza skarg. Europejski Inspektor Ochrony Danych zbada wniesioną skargę i poinformuje skarżącego, czy ją podtrzymuje – a jeśli tak, to w jaki sposób problem zostanie rozwiązany. Jeśli skarżący **nie zgadza się** z opinią Inspektora, może wnieść sprawę do Trybunału Sprawiedliwości UE.

### **Źródła:**

Podręcznik europejskiego prawa o ochronie danych, Agencja *Praw Podstawowych Unii Europejskiej*; Rada Europy

Ochrona danych, Komisja Europejska

[https://edps.europa.eu/edps-homepage\\_en?lang=pl](https://edps.europa.eu/edps-homepage_en?lang=pl)

[http://www.europarl.europa.eu/atyourservice/pl/displayFtu.html?ftuId=FTU\\_5.12.8.html](http://www.europarl.europa.eu/atyourservice/pl/displayFtu.html?ftuId=FTU_5.12.8.html)

### **Przygotował:**

**Punkt Informacji Europejskiej**

**Europe Direct – Poznań**

przy Wielkopolskiej Izbie Rzemieślniczej w Poznaniu

al. Niepodległości 2, 61-874 Poznań

tel. 61 8521670

e-mail: [europedirect-poznan@irpoznan.com.pl](mailto:europedirect-poznan@irpoznan.com.pl), [www.europe-direct.poznan.pl](http://www.europe-direct.poznan.pl)

Projekt współfinansowany ze środków Komisji Europejskiej

