

# OCHRONA DANYCH OSOBY

---

O CO TYLKO HAŁASU?

# CZYM WŁAŚCIWIE SĄ DANE OSOBOWE?

---

- Dane osobowe to informacje, dzięki którym możliwe jest zidentyfikowanie osoby fizycznej.
- Do danych osobowych możemy zaliczyć m.in. :
  - imię i nazwisko
  - adres
  - numer PESEL
  - numer NIP

# CZYM WŁAŚCIWIE SĄ DANE OSOBOWE?

---

- Do danych osobowych zalicza się również dane pozajęzykowe jak np.:
  - obraz
  - dźwięk
  - odciski palców
  - informację o kodzie genetycznym.
- Przykładem danych osobowych są również adresy e-mail, jeśli dzięki nim można zidentyfikować daną osobę

# CZY WIESZ ŻE...?

---

- Dane osobowe są cennym „towarem” rynkowym wykorzystywanym w celach marketingowych i sprzedażowych.

# NIESTETY CZASAMI ZDARZA SIĘ ŻE...

---

- Aby zdobyć informacje o Tobie i Twoich danych osobowych, przestępcy mogą wykorzystywać skomplikowane techniki informatyczne lub środki socjotechniczne.
- W przypadku utraty danych osobowych, kiedy posługuje się nimi osoba do tego nieuprawniona, dane te mogą zostać użyte w celach przestępczych, takich jak np. wyłudzenie pożyczek czy kredytów.

# JEDNAK MOŻESZ COŚ ZROBIĆ...

---

- Mimo że nie jesteś w stanie ochronić swoich danych w 100%, możesz zrobić wiele aby ograniczyć ryzyko ich wykorzystania (nie tylko w celach przestępczych, ale przede wszystkim dla ochrony swojej prywatności).

---

**KILKA RAD KTÓRE POMOGĄ CI CHRONIĆ  
SWOJE DANE OSOBOWE I UNIKNAĆ  
PROBLEMÓW**

# UWAŻAJ NA TO CO I KOMU UDOSTĘPNIASZ O SOBIE W INTERNECIE

---

- **Ogranicz udostępnianie Twoich danych w Internecie.**
- Internet a w szczególności media społecznościowe mogą być kopalnią wiedzy o Tobie, Twoim stanie majątkowym, miejscu pracy, wydarzeniach z Twojego codziennego życia, Twoich poglądach czy zainteresowaniach.
- Dane te są cenne nie tylko dla działów marketingu różnych firm, po to by na Twoich zachowaniach w sieci oprzeć kierowaną ofertę, ale niekiedy i dla przestępców.
- Jeżeli Twój profil jest w pełni publiczny, możesz być narażony na użycie Twoich danych bez Twojej wiedzy i przyzwolenia niezgodnie z celami, dla których je udostępniłeś.



# NIE ZOSTAWIAJ DOKUMENTÓW W ZASTAW

---

- **Nigdy nie oddawaj w zastaw dowodu osobistego**, paszportu, prawa jazdy, legitymacji szkolnej lub studenckiej. Warto pamiętać, że zgodnie z prawem zatrzymywanie dowodu osobistego bez podstawy prawnej jest karane.
- Utrata kontroli nad dowodem osobistym naraża Cię na posłużenie się tym dokumentem bez Twojej wiedzy i woli, co z kolei stwarza niebezpieczeństwo kradzieży tożsamości. Osoby dysponujące kompletem informacji o Tobie, czy kopią Twojego dokumentu tożsamości, mogą podszyć się pod Ciebie i np. dokonywać na Twoją szkodę różnych transakcji, takich jak zaciągnięcie kredytu w banku, wypożyczenie drogiego sprzętu i niezwrócenie go lub zawarcie w Twoim imieniu różnego rodzaju umów, np. z zakresu usług telekomunikacyjnych, z dalszymi obciążającymi Cię konsekwencjami.

# NIE POZWALAJ NA KOPIOWANIE DOKUMENTÓW TOŻSAMOŚCI

---

- Co do zasady nie powinieneś się godzić na kopiowanie Twojego dokumentu tożsamości.
- Tylko w niektórych sytuacjach jest to wyjątkowo dopuszczalne, gdy pozwalają na to przepisy.

# NIE PODAWAJ DANYCH PRZEZ TELEFON

---

- **Unikaj przekazywania danych telefonicznie** – szczególnie, gdy to nie Ty inicjujesz rozmowę, ale ktoś dzwoni do Ciebie.
- Udostępnianie danych na odległość obarczone jest ryzykiem, brakiem pewności co do tego komu faktycznie dane są przekazane. Nie daj się zaskoczyć, sprowokować do udostępniania danych wbrew Twojej woli, dla nieznanych, niewyjaśnionych przez rozmówcę celów.
- Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

# UWAŻAJ NA RÓŻNE FORMULARZE, POPRZEZ KTÓRE UDOSTĘPNIASZ DANE

---

- Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów.
- Zastanów się czy faktycznie chcesz założyć kartę lojalnościową w sklepie. W takich sytuacjach podajesz sklepom imię, nazwisko, adres zamieszkania, datę urodzenia, adres e-mail, numer telefonu.
- Nie podawaj wszelkich danych, które pozwalają na pełną identyfikację, jeżeli w danej sytuacji nie jest to konieczne.

# UWAŻAJ NA ZGODY KTÓRE PODPISUJESZ

---

- **Zanim zaznaczysz wszystkie zgody, upewnij się czego dotyczą.**
- Zwróć uwagę czy w formularzu zgody nie są zaznaczone domyślnie. Zgodnie z prawem nie powinno tak być. Dokładnie czytaj, czego dotyczą klauzule zgód.
- Pamiętaj, że wyrabiając kartę lojalnościową często udzielasz zgód na wykorzystywanie danych w celach marketingowych nie tylko administratora, ale i jego partnerów biznesowych. O ile możesz, zweryfikuj, kim oni są, jakie to są firmy. Zgody na marketing „cudzy” powinny być nieobowiązkowe, powinna być Ci pozostawiona możliwość wyboru co do tego, czy taką zgodę wyrazisz.

# OBOWIĄZEK INFORMACYJNY

---

- Pamiętaj, że administrator musi spełnić wobec Ciebie obowiązek informacyjny, czyli przekazać Ci niezbędne informacje na swój temat, podając m.in. swoją tożsamość, dane kontaktowe oraz dane kontaktowe swojego inspektora danych osobowych (o ile go wyznaczył), a także cel i podstawę prawną przetwarzania danych.
- W przypadku wątpliwości, zadawaj pytania administratorom. Powinni Cię poinformować o okresie przez jaki dane będą przetwarzane oraz o przysługujących Ci prawach, w tym dostępu do danych, ich sprostowania, usunięcia czy wniesienia sprzeciwu wobec przetwarzania, a także, czy Twoje dane będą komuś innemu (innym odbiorcom) przekazywane.
- Administrator powinien Ci zapewnić, by możliwość wycofania zgody była równie łatwa, jak jej udzielenie oraz powinieneś być poinformowany o prawie do cofnięcia zgody nim ją wyrazisz.

# NIE WYRZUCAJ DANYCH NA ŚMIETNIK, DOPÓKI ICH NIE ZNISZCZYSZ

---

- **Zanim wyrzucisz dokumenty do kosza, zniszcz je** w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.
- Wszelkie dokumenty z Twoimi danymi to kolejne źródło wiedzy o Tobie.
- Faktury, rachunki, zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach zawierają wiele różnych informacji umożliwiających wyciągnięcie wniosków na Twój temat, np. ustalenie tego, gdzie pracujesz, ile zarabiasz, kiedy nie ma Cię w domu, ile masz dzieci czy jak drogie robisz zakupy.

# USUWAJ TRWALE DANE Z NOŚNIKÓW

---

- Zanim pozbędziesz się starych dysków twardych, kart pamięci, pendrive'ów czy innych nośników, trwale usuń z nich dane.
- Pamiętaj, że zwykłe skasowanie danych nie będzie wystarczające, ponieważ wiele danych da się odzyskać. Zanim wyrzucisz nośnik albo go sprzedasz, usuń z niego dane, korzystając z odpowiedniego oprogramowania.
- Coraz więcej informacji na Twój temat jest zapisanych w komputerach, smartfonach, aparatach fotograficznych czy tabletach.
- Zanim się ich pozbędziesz, przywróć ustawienia fabryczne urządzeń, aby nie było w nim zapamiętanych loginów i haseł do różnych usług i aplikacji, z których korzystałeś, a zwłaszcza z takich, z których nadal korzystasz.



# UŻYWAJ PROGRAMÓW CHRONIĄCYCH KOMPUTER

---

- Używaj oprogramowania chroniącego komputer i urządzenia mobilne przed niepożądanymi działaniami z zewnątrz, np. złośliwego oprogramowania.
- Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall.

# BĄDŹ CZUJNY W SIECI

---

- **Nie odpowiadaj na maile od osób, których nie znasz** np. tzw. spamerów, zwłaszcza gdy domagają się podania jakichś informacji o tobie czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika, sugerują zmianę identyfikatora i hasła.
- **Zachowaj ostrożność przy korzystaniu z usług bankowości elektronicznej.** Zwracaj uwagę czy aby na pewno logujesz się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL (widoczny w pasku adresu przeglądarki).

# RÓB ROZSĄDNIIE ZAKUPY PRZEZ INTERNET

---

- **Zachowaj ostrożność przy dokonywaniu zakupów przez Internet.** Weryfikuj sklepy, w których chcesz coś kupić: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego.
- Jeśli masz wątpliwości co do bezpieczeństwa Twoich danych zastanów się czy koniecznie musisz dokonać zakupów u tego sprzedawcy. Weryfikuj regulaminy i polityki prywatności – unikaj sprzedawców nieprzedstawiających takich dokumentów czy też prezentujących w nich postanowienia zbyt ogólne, niejasno czy nieprecyzyjnie brzmiące, sformułowane niepoprawnie gramatycznie czy językowo, może to bowiem oznaczać, że są to podmioty niepodlegające polskiemu czy europejskiemu prawu.

# ZMIENIAJ HASŁA

---

- **Okresowo zmieniaj hasła dostępu** nie tylko do swojego komputera, poczty elektronicznej, systemów bankowości elektronicznej ale nawet sklepów internetowych, w których -masz konto użytkownika.
- Staraj korzystać z różnych haseł. Najlepiej, aby nie miały one nic wspólnego z Twoimi życiem osobistym, miejscem zamieszkania, Twoim imieniem i nazwiskiem, datą urodzin, imionami Twoich bliskich czy Twoich zwierząt.

---

**PAMIĘTAJ,  
ZACHOWUJĄC ZDROWY ROZSĄDEK  
PODCZAS UDOSTĘPNIANIA SWOICH  
DANYCH OSOBOWYCH  
CHRONISZ SIEBIE I SWOICH BLISKICH.**

# ŹRÓDŁA:

---

- <https://uodo.gov.pl/pl/138/1221>
- <https://www.poradyodo.pl/nowosci-rodo/uodo-uczy-jak-chronic-swoje-dane-osobowe-9409.html>
- [http://osobowedane.pl/dane-osobowe/?gclid=EAlaIQobChMI5fVWR5ti87gIV2OF3Ch2pBgcKEAAYASAAEgId2PD\\_BwE](http://osobowedane.pl/dane-osobowe/?gclid=EAlaIQobChMI5fVWR5ti87gIV2OF3Ch2pBgcKEAAYASAAEgId2PD_BwE)