POZNAJ PRAWA I WARTOŚCI UNII EUROPEJSKIEJ

- grant realizowany przez Fundację REYBUDHELP w ramach projektu grantowego „Wzmacniamy Europę SPLOTowymi wartościami” współfinansowanego ze środków Programu Komisji Europejskiej CERV „Obywatele, Równość, Prawa i Wartości” na lata 2021 – 2027

Dofinansowane przez Unię Europejską

REYBUDHELP

sieć splot wartości

Cz. 7

Ochrona danych osobowych

Karta Praw Podstawowych

TYTUŁ II
WOLNOŚCI

Artykuł 8
Ochrona danych osobowych

1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.
2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.
3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

PRYWATNOŚĆ I DANE OSOBOWE

Dane osobowe to część naszej prywatności.
Dane osobowe to każda informacja umożliwiająca identyfikację konkretnej osoby, np. imię i nazwisko, PESEL, adres, data urodzenia, głos, wizerunek.
Dane szczególnie chronione to np. odcisk palca, informacja o nałogach czy zdrowiu.

Zgodnie z prawem wszystkie dane osobowe zasługują na ochronę.

Dane wrażliwe (szczególnie chronione)

pochodzenie rasowe lub etniczne

poglądy polityczne

przekonania religijne lub filozoficzne

stan zdrowia

kod genetyczny

nałogi

życie seksualne

przynależność wyznaniowa, partyjna lub związkowa

skazania, orzeczenia o ukaraniu

mandaty, orzeczenia wydane przed sądem lub urzędem

Przetwarzanie danych osobowych to wszystkie operacje, jakim poddawane są informacje, w szczególności:

- zbieranie (gromadzenie)
- przechowywanie
- udostępnianie
- zmienianie
- przekazywanie
- utrwalanie
- opracowywanie
- usuwanie (niszczenie, modyfikacja)

W związku z szybkim postępem technologicznym Unia Europejska przyjęła nowe przepisy
– ogólne rozporządzenie o ochronie danych tzw. RODO, aby dostosować regulacje prawne do ery cyfrowej.

Unijne ogólne rozporządzenie o ochronie danych tzw. **RODO** to **najostrzejsze na świecie przepisy o ochronie prywatności i bezpieczeństwie danych**.

RODO definiuje:

- prawa podstawowe osób fizycznych w epoce cyfrowej
- obowiązki podmiotów przetwarzających dane
- sposoby zapewniania przestrzegania przepisów
- kary dla naruszających przepisy

Prawa osób fizycznych

Prawa te są szersze niż w poprzednich aktach prawnych – dają osobom większą kontrolę nad dotyczącymi ich informacjami.

Osoby te mogą m.in.:

- decydować, czy ich dane wolno przetwarzać (wymóg zgody na przetwarzanie)
- mieć łatwiejszy dostęp do swoich danych osobowych
- zażądać sprostowania lub usunięcia danych (prawo do „bycia zapomnianym”)
- sprzeciwić się np. wykorzystywaniu danych osobowych do profilowania
- przenieść dane do innego usługodawcy.

Obowiązki firm i organizacji

RODO określa ogólne obowiązki administratora danych i podmiotu przetwarzającego te dane w jego imieniu.
Muszą oni m.in. wdrożyć środki bezpieczeństwa odpowiednie do ryzyka, które wiąże się z wykonywanymi przez nich operacjami przetwarzania.
Wszystkie organy publiczne, a spośród firm – te, które dokonują operacji przetwarzania wrażliwych danych osobowych **– muszą wyznaczyć inspektora ochrony danych**.

MASZ „PRAWO DO BYCIA ZAPOMNIANYM”

„Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe (…)”
art. 17 ust. 1 RODO

Jakie są podstawy prawne do przetwarzania danych osobowych?

- osoba, której dane dotyczą, wyrazi na to ZGODĘ, chyba, że chodzi o usunięcie danych
- niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa
- 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
- niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego
- niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą

Przetwarzanie danych jest dopuszczalne

- **przetwarzanie dotyczy danych, które są niezbędne do:** dochodzenia praw przed sądem, do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych;
- **przetwarzanie dotyczy danych**, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą - prowadzenie badań naukowych;
- **do wykonania statutowych zadań** kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, 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.

Warunki przetwarzania danych osobowych

Pracownik może przetwarzać dane, tylko i wyłącznie w sytuacji, gdy:

- posiada pisemne **upoważnienie** do przetwarzania danych osobowych
- jest umieszczony **w Ewidencji Osób Upoważnionych** do przetwarzania danych
- w **celu i zakresie** wskazanym w upoważnieniu
- przez **okres** na jaki upoważnienie zostało udzielone.

Uwaga!

Pracownicy upoważnieni do przetwarzania danych osobowych są zobowiązani do ochrony danych zarówno w trakcie trwania zatrudnienia, jak i po jego ustaniu.

Zgodnie z art. 4 pkt 7 rozporządzenie RODO pojęcie **administrator danych osobowych** oznacza organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych.

W przypadku osób prowadzących działalność gospodarczą to sam przedsiębiorca pełni funkcję **ADO**, czyli **administratora danych osobowych**.

Jednym z najważniejszych zadań, które może wykonywać administrator danych osobowych jest powołanie **Inspektora Ochrony Danych Osobowych (IODO)** - jeśli przepisy go do tego zobowiązują.

Do wyznaczenia IOD zobowiązane są podmioty publiczne, podmioty przetwarzające na dużą skalę dane wrażliwe oraz podmioty, których główna działalność polega na monitorowaniu osób na dużą skalę.
Pozostałe podmioty również mogą wyznaczyć IOD, jednak nie jest to dla nich obowiązkowe.

Urząd Miasta Rejowiec Fabryczny

Inspektor Ochrony Danych Osobowych

Pani Katarzyna Żółkiewska - Malicka

adres e-mail: katarzyna.zolkiewska@zeto.lublin.pl

tel. 609 389 097

JAK ZAPEWNIĆ SOBIE BEZPIECZEŃSTWO W CYFROWYM ŚWIECIE I ZWIĘKSZYĆ KONTROLĘ NAD SWOIMI DANYMI W SIECI?

1. Stosuj zabezpieczenia programowe i fizyczne swoich urządzeń.
2. Ograniczaj informacje na swój temat w Internecie.

Im więcej korzystasz z sieci, tym więcej uwagi poświęcaj ochronie danych osobowych i prywatności w sieci.

O CZYM WARTO PAMIĘTAĆ, ABY CHRONIĆ SWOJE DANE?

1

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

• Zdarza się, że sami nadmiernie dzielimy się informacjami na nasz temat. Media społecznościowe mogą być kopalnią wiedzy o Tobie, Twoim stanie majątkowym, miejscu nauki, zamieszkania, przebywania, poglądach i zainteresowaniach.

• **Unikajmy dzielenia się informacjami dot. zdrowia** i udostępniania innych danych, które powinny być szczególnie chronione.

• Im więcej korzystamy z serwisów społecznościowych, tym bardziej **dbajmy o restrykcyjne ustawienia ochrony naszej prywatności**.

2

NIE ZOSTAWIAJ DOKUMENTÓW W ZASTAW

• Nie pozostawiaj dowodu osobistego, paszportu, prawa jazdy, legitymacji szkolnej lub studenckiej jako zastaw. Nikt zgodnie z prawem nie może tego od Ciebie wymagać. Utrata kontroli nad dokumentem tożsamości naraża Cię na niebezpieczeństwo.

3

CZYTAJ KLAUZULE INFORMACYJNE I POLITYKI PRYWATNOŚCI,

aby mieć świadomość, w jaki sposób i na jakich warunkach przetwarzane są Twoje dane.

4

PAMIĘTAJ O OCHRONIE WIZERUNKU

- Udostępniając swój wizerunek zwróć uwagę czy zdjęcie nie będzie kompromitowało Cię w przyszłości lub nie zdradza zbyt wiele informacji prywatnych o Tobie i osobach bliskich czy danych szczególnie chronionych.
- **Jeśli chcesz udostępnić zdjęcie innej osoby zapytaj o zgodę.**

5

WYLOGUJ SIĘ Z KONTA

• Po zakończonej pracy w różnych serwisach i portalach zawsze **się wyloguj.** Gdy się nie wylogujemy, osoba, która usiądzie przy komputerze, może wykonać operacje z wykorzystaniem naszych danych osobowych.

• Nie loguj się do kont korzystając z otwartych **sieci Wi-Fi**.

6

NIE PODAWAJ DANYCH PRZEZ TELEFON

• Unikaj przekazywania danych telefonicznie – szczególnie, gdy ktoś dzwoni do Ciebie. Upewnij się komu udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt.

7

UWAŻAJ NA FORMULARZE Z DANYMI

• Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Pamiętaj, że administrator danych musi spełnić wobec Ciebie **obowiązek informacyjny**, czyli przekazać Ci informacje na swój temat tak, abyś miał pewność, przez kogo i w jakim celu dane będą przetwarzane.

• Przy wypełnianiu formularzy podawaj tylko te dane, które są konieczne.

8

NIE WYRZUCAJ DANYCH NA ŚMIETNIK

Dokumenty z Twoimi danymi, to skarbnica wiedzy o Tobie, zwłaszcza gdy zawierają m.in. informacje o tym, gdzie pracujesz, ile zarabiasz, kiedy nie ma Cię w domu. Dlatego zniszcz je w sposób uniemożliwiający odtworzenie, zawartych w nich danych osobowych, zanim wyrzucisz je do kosza.

9

USUWAJ TRWALE DANE Z NOŚNIKÓW

Zanim pozbędziesz się starych dysków twardych, pendrive'ów, kart pamięci, etc. usuń z nich swoje dane. Aby trwale usunąć dane, skorzystaj z odpowiedniego do tego oprogramowania.

10

UŻYWAJ PROGRAMÓW CHRONIĄCYCH URZĄDZENIA

Systematycznie aktualizuj oprogramowanie. Oprócz popularnych programów antywirusowych przydatne może być oprogramowanie zabezpieczające przed ingerencją z zewnątrz tzw. firewall.

11

BĄDŹ CZUJNY W SIECI

- **Nie odpowiadaj na maile od nieznanych Ci osób/instytucji**, gdy domagają się podania jakichś informacji czy namawiają Cię do kliknięcia w przesłany link lub otwarcia załącznika.
- Przy korzystaniu z usług bankowości elektronicznej **zwracaj uwagę czy strona banku ma certyfikat SSL.** Klikając w ikonę po lewej stronie adresu (zazwyczaj będzie to symbol kłódki), możemy sprawdzić, na kogo jest wystawiony certyfikat.

12

DBAJ O SILNE HASŁA I NIE UDOSTĘPNIAJ ICH NIKOMU

• Okresowo **zmieniaj hasła** dostępu do komputera, poczty elektronicznej, systemów bankowości elektronicznej, ale również sklepów internetowych szczególnie w przypadku podejrzenia, że nastąpił wyciek danych z firmy i hasło zostało ujawnione.

• Korzystaj z **różnych haseł** do gier, komunikatorów, poczty elektronicznej i serwisów społecznościowych. Najlepiej, aby nie miały one nic wspólnego z Twoimi imieniem i nazwiskiem, datą urodzin itp.

• Uaktywnij **dwuskładnikowe uwierzytelnianie** i stosuj unikalną kombinację haseł, w celu uzyskania dostęp do systemu/urządzenia.

13

OSTROŻNIE INSTALUJ POTRZEBNE APLIKACJE Z ZAUFANYCH ŹRÓDEŁ

Instalując aplikacje, gry i programy, szczególnie na tablecie lub smartfonie, nieświadomie możemy np. pozwolić na dostęp do listy kontaktów, zdjęć, danych o lokalizacji.

Uważnie czytajmy komunikaty poprzedzające instalację i zwracajmy uwagę do jakich danych instalowana aplikacja będzie miała dostęp i czy to jest konieczne do realizacji usługi.

14

NIE PODAWAJ WSZELKICH DANYCH, KTÓRE POZWOLĄ NA TWOJĄ PEŁNĄ IDENTYFIKACJĘ

Zakładając kartę lojalnościową podajesz sklepom imię, nazwisko, adres zamieszkania, datę urodzenia, adres e-mail i nr telefonu, w zamian za promocje i bony rabatowe.

Często niestety udzielasz zgód na wykorzystywanie Twoich danych w celach marketingowych, nie tylko sprzedawcy, ale i jego partnerom.

Dzień Ochrony Danych Osobowych jest obchodzony 28 stycznia.

DZIĘKUJĘ ZA UWAGĘ

KRYSTYNA ZERA

FUNDACJA REYBUDHELP