

DODATEK SPECJALNY "TORNISTRA"

STYCZEŃ 2020

Ochrona Danych Osobowych

opr. Pani Izabela Borucińska

DWA WAŻNE WYDARZENIA ZWIĄZANE Z OCHRONĄ DANYCH OSOBOWYCH I BEZPIECZEŃSTWEM CYFROWYM

9 lutego – Dzień Bezpiecznego Internetu

Dzień Bezpiecznego Internetu (DBI) obchodzony jest z inicjatywy Komisji Europejskiej od 2004 roku. To okazja to inicjowania i propagowania działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych.

Początkowo wydarzenie to świętowały jedynie państwa europejskie, ale już od lat DBI przekracza granice Europy angażując państwa z całego świata.



28 stycznia – Dzień Ochrony Danych Osobowych

Dzień Ochrony Danych powstał z inicjatywy Komitetu Ministrów Rady Europy. Obchody przypadają w rocznicę sporządzenia Konwencji 108 Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych. Konwencja jest najstarszym

aktem prawnym o zasięgu międzynarodowym, który reguluje kwestie dotyczące ochrony danych osobowych.

Dzień Ochrony Danych Osobowych ma na celu zwrócenie uwagi na zagadnienia związane z ochroną danych oraz podniesienie świadomości w tym zakresie. W tym dniu, w całej Europie, odbywają się różnorodne



spotkania, konferencje, warsztaty, konkursy i wystawy uświadamiające, jak niebezpieczne skutki przynieść może nieuwaga lub zbyt duża niefrasobliwość w udostępnianiu naszych danych osobowych. W czasach dynamicznego rozwoju nowych technologii informacja, a co za tym idzie informacja o nas, jest niezwykle cenna i narażona na niewłaściwe wykorzystanie. **Jesteśmy odpowiedzialni za nasze dane, dlatego tak ważne jest podnoszenie świadomości w tym zakresie.** Coraz częściej i coraz chętniej, nie zdając sobie sprawy z płynących zagrożeń, udostępniamy dane o nas oraz naszych bliskich.

Rozporządzenie unijne, które od 25 maja 2018 roku zaczęło obowiązywać we wszystkich państwach członkowskich UE stało się strażą praw osób, których dane dotyczą. **Znajomość przepisów jest bardzo ważna, ponieważ mając świadomość, kiedy i dlaczego udostępniamy swoje dane, będziemy mogli mieć wpływ na to, co się z nimi dzieje i w jaki sposób są wykorzystywane. Wyznaczenie granicy w udostępnianiu informacji o nas samych jest tutaj kluczowe.**

Polska włączyła się w organizację Dnia Ochrony Danych Osobowych w roku 2007 roku.

W 2021 roku będziemy zatem świętować ten dzień po raz piętnasty.

CO TO SĄ DANE OSOBOWE?

Ochrona danych osobowych jest częścią tzw. **prawa do prywatności**, które jest jednym z praw człowieka oraz dobrem osobistym. Ochrona prywatności jest szczególnie istotnym zagadnieniem w społeczeństwie informacyjnym.

Z jednej strony warto chronić swoją prywatność i dbać o swoje bezpieczeństwo poprzez pilnowanie dostępu do informacji o sobie.

Z drugiej strony jednak funkcjonowanie we współczesnym świecie opiera się na wymianie informacji – na ujawnianiu swoich poglądów, zainteresowań i faktów z życia.

Zgodnie z obowiązującym prawem **dane osobowe** to wszelkie informacje dotyczące konkretnej osoby – zidentyfikowanej (np. takiej, którą znamy osobiście) lub możliwej do zidentyfikowania (czyli takiej, którą można wskazać na podstawie posiadanych informacji, choćby numeru identyfikacyjnego, wyglądu lub jakiejkolwiek kombinacji cech, np. dziewczynka, która ma na imię Marcjanna, nosi okulary i chodzi do konkretnej szkoły i klasy).

Daną osobową może być każda informacja, nie tylko imię i nazwisko, ależ też np. informacja o odwiedzanych stronach internetowych, czy ocenach z matematyki.

Informacja, która dotyczy instytucji (np. firmy, szkoły), grupy osób, osoby zmarłej lub fikcyjnej (np. postaci literackiej) – nie jest daną osobową.

To, czy jakaś informacja jest daną osobową, zależy od okoliczności.

Na przykład: tablice rejestracyjne samochodu dla policji są daną osobową, bo policja bez trudu może w bazie danych zweryfikować, kto jest właścicielem auta, ale dla innego kierowcy, który nie ma takiej możliwości – już nie.

Dane osobowe, o których wspomniano powyżej, to **zwykle dane osobowe**.

Natomiast dane osobowe wrażliwe, nazywane w RODO danymi szczególnych kategorii, które dotyczą spraw intymnych, należą do grupy danych szczególnie chronionych.

Szczególne kategorie danych osobowych to dane ujawniające:

- Pochodzenie rasowe lub etniczne,
- Poglądy polityczne,
- Przekonania religijne lub światopoglądowe,
- Przynależność do związków zawodowych,
- Dane genetyczne,
- Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- Dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

Tych danych, co do zasady, nie wolno przetwarzać. Jest to możliwe jedynie w ściśle określonych w prawie przypadkach (np. przychodnie zdrowia, szpitale przetwarzają dane o stanie zdrowia pacjentów) lub za pisemną zgodą osoby, której dane wrażliwe dotyczą.



KTO TO JEST ADMINISTRATOR DANYCH OSOBOWYCH?

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

Na przykład w szkole administratorem danych osobowych jest szkoła, na której czele stoi i ją reprezentuje dyrektor szkoły.

Administrator odpowiada za to, by przetwarzanie danych odbywało się zgodnie z prawem i było odpowiednio zabezpieczone.

Administrator ma obowiązek informować osoby, których dane przetwarza, jakie dane przechowuje i jak je wykorzystuje, musi także udostępnić informacje o sobie i podać swoje dane kontaktowe (jest to tzw. **obowiązek informacyjny**).

Dane osobowe podlegają ochronie, co oznacza, że podmioty, które chcą je przetwarzać (tzn. osoby, firmy, instytucje publiczne), powinny spełnić określone warunki. Szczególnie chronione są **dane wrażliwe**.

CO KRYJE SIĘ POD POJĘCIEM „PRZETWARZANIE DANYCH”?

Przetwarzanie danych to wszystkie czynności, które „wykonujemy” na danych osobowych: ich zbieranie, utrwalanie, przechowywanie (archiwizowanie), opracowywanie, poprawianie, udostępnianie a także usuwanie, również operacje wykonywane w systemach informatycznych.

Przykładem przetwarzania może być gromadzenie danych osobowych ucznia w dziennikach – papierowych lub elektronicznych – uzupełnianie tych danych o nowe, pozyskane informacje (np. oceny), aktualizacja, kiedy np. ktoś zmieni adres zamieszkania, czy usuwanie, kiedy uczeń przeniesie się do innej szkoły.

Aby instytucja mogła zgodnie z prawem przetwarzać dane osobowe musi posiadać tzw. podstawę przetwarzania danych. Dzięki tej podstawie będzie mogła legalnie dokonywać na danych osobowych tych operacji, które są ważne dla jej działalności.



KIEDY PRZETWARZANIE DANYCH JEST LEGALNE?

Nikt – ani pracownik firmy, ani urzędnik państwowy, ani policjant – nie może przetwarzać naszych danych bez podstawy

prawnej. Ustawa wskazuje konkretne sytuacje, w których jest to dozwolone. Najczęściej wykorzystywane, to:

- **zgoda osoby**, której dane dotyczą (musi być dobrowolna; w drobnych, codziennych sprawach mogą ją wyrażać osoby **powyżej 13 roku życia**; w innych przypadkach – tylko osoby dorosłe);

- **przepis prawa** (np. szkoła ma prawo przetwarzać dane uczniów w celach związanych z ich kształceniem; firma ma prawo przetwarzać dane swoich pracowników);

- **fakt, że dane są niezbędne do wykonania umowy** (np. adres wysyłki w przypadku zakupów w sklepie internetowym).

Zgoda na przetwarzanie danych osobowych powinna dotyczyć konkretnego administratora danych i konkretnego celu. Żeby przetwarzać dane w innym celu, trzeba uzyskać osobną zgodę. Na przykład, jeśli wyrazisz zgodę na przetwarzanie swoich danych w ramach udziału w konkretnym konkursie – organizator nie ma prawa wykorzystać informacji ze zgłoszenia w kolejnej edycji tego konkursu. Nie może też przekazać Twoich danych komuś innemu, kto np. chciałby wysyłać katalogi reklamowe o książkach (chyba, że również na to wyrazisz zgodę).

Każdej osobie, której dane są przetwarzane, przysługują w związku z tym konkretne uprawnienia:

- **prawo do informacji** o tym, skąd dany podmiot pozyskał dane i w jakim celu je przetwarza, np. jeśli dzwoni do Ciebie telemarketer, możesz oczekiwać informacji, skąd ma Twój numer telefonu, kto i w jakim celu go wykorzystuje;

- **prawo do wycofania zgody**, jeśli po pewnym czasie zmieniłeś zdanie, np. jeśli podałeś swój adres e-mail jakiejś organizacji lub stowarzyszeniu, ale nie chcesz już otrzymywać ich newsletterów, możesz napisać do nich, by zaprzestali przetwarzania Twoich danych;

- **prawo do uzupełnienia, uaktualnienia i sprostowania danych** – jeśli Twoje dane się zmieniły lub są niezgodne z prawdą, możesz je zaktualizować;

- jeśli ktoś legalnie przetwarza Twoje dane, ale nie odbywa się to na podstawie żadnej z trzech wskazanych wyżej podstaw prawnych (a np. na podstawie usprawiedliwionego interesu

administratora), możesz zgłosić sprzeciw i żądać zaprzestania przetwarzania danych.

Każdy może mieć wpływ na to, jakie informacje o nim są ujawniane i wykorzystywane.

PORADY DLA UŻYTKOWNIKÓW PORTALI O CZYM POWINNIŚMY PAMIĘTAĆ?

- **Internet jest pamiętliwy!** Zachowaj ostrożność w dzieleniu się informacjami o sobie – cokolwiek napiszesz na swój temat lub na temat innych osób, usunięcie takiej informacji i wszystkich powielonych jej kopii z sieci Internet jest bardzo trudne lub wręcz niemożliwe.

- **Bądź ostrożny w nawiązywaniu znajomości w sieci** – tak jak w życiu - osoby, które poznajesz w sieci, mogą nie być tymi, za które się podają i wcale nie muszą chcieć być Twoimi przyjaciółmi.

- Zanim zdecydujesz się zapisać do portalu społecznościowego, **zapoznaj się z jego regulaminem i sprawdź możliwość kontaktu z jego administratorem** – jeśli informacje będą niepełne lub nie będą spełniały Twoich standardów prywatności, nie zapisuj się!

- Zastanów się jakie informacje o sobie umieszczasz w sieci. **Czy chciałbyś, aby te informacje były znane Twoim rodzicom, nauczycielom, kolegom...?**

- Podczas rejestracji w portalu i późniejszego korzystania z niego, **nie wpisuj swoich pełnych danych osobowych** – wystarczy, że wpiszesz tylko te, które pomogą Twoim faktycznym znajomym w łatwym odnalezieniu Ciebie.

- Rejestrując się w portalu **staraj się używać innych identyfikatorów i haseł**, niż te, które wykorzystujesz do ważnych usług np. serwisu bankowości internetowej.

- Celem podniesienia Twojego bezpieczeństwa w portalu **staraj się używać bezpiecznych haseł i okresowo je zmieniaj**. Bezpieczne hasło zbudujesz przy łącznym użyciu znaków z grup małych i dużych liter, cyfr i znaków specjalnych. Unikaj haseł trywialnych takich jak: Twoje imię, imię psa, data

urodzenia itp. Pamiętaj, że hasło dzisiaj uważane za bezpieczne może nie być takim w przyszłości.

- **Publikując zdjęcia** z własnym wizerunkiem lub z wizerunkami innych osób musisz mieć świadomość, że **znacznie ułatwiasz identyfikację siebie i innych** oraz możesz przekazać w ten sposób znacznie więcej informacji niż zdajesz sobie sprawę.

- Podając w portalu społecznościowym informacje o innej osobie oraz publikując jej zdjęcia, **upewnij się, że ta osoba nie ma nic przeciwko takiej publikacji.**

- **Korzystaj z opcji umożliwiających ograniczenie kręgu osób**, którym informacje o Tobie będą udostępniane.

RADY TAKŻE DLA DOROSŁYCH, MOŻNA POKAZAĆ RODZICOM

- Nie udostępniaj danych osobowych niepowołanym osobom;
- Bardzo dokładnie niszczone stare dokumenty i korespondencję, których chcesz się pozbyć – to fantastyczne źródło wiedzy na Twój temat;

- Nie zgadzaj się na spisywanie danych z dowodu osobistego, lub innych dokumentów przez niepowołane osoby;

- Nie zostawiaj swoich dokumentów w tzw. depozycie – np. wypożyczając sprzęt sportowy;

- Nie podawaj swoich danych w trakcie rozmów telefonicznych nieznajomym osobom;

- Nigdy nie otwieraj e-maili podejrzanych lub nieznanego pochodzenia.

ZASADY POSTĘPOWANIA, KTÓRE POMOGĄ CZUĆ SIĘ BEZPIECZNIE W SIECI

- 1.** Nigdy nie podawaj informacji o sobie, takich jak: Twój adres, numer telefonu, miejsce pracy i numer do rodziców oraz nazwy i miejsce Twojej szkoły.

- 2.** Mów swoim rodzicom wszystko, co sprawiło, że czujesz się zakłopotany, kiedy używałeś Internetu.

- 3.** Nigdy bez zgody rodziców nie umawiaj się na spotkanie z kimś, kogo poznałeś, w Internecie.

Jeżeli rodzice zgodzą się na spotkanie, upewnij się, że odbędzie się w miejscu publicznym i nie idź tam sam.

4. Nigdy nie odpowiadaj na wiadomości z sieci, które są dwuznaczne, nieprzyzwoite, agresywne, przerażające albo wywołujące u ciebie zmieszanie. Zrób kopię takiej wiadomości i przekaz rodzicom.

5. Nigdy bez zgody rodziców nie wysyłaj własnych zdjęć ani innych prywatnych materiałów osobie, którą poznałeś w Internecie.

6. W Internecie znajdują się także strony przeznaczone tylko dla dorosłych. Jeżeli sam znajdziesz taką stronę, opuść ją – to nie jest strona dla Ciebie.

7. Przestrzegaj reguł, dotyczących korzystania z Internetu, jakie ustali Twoi rodzice.



Stosuj reguły **SMART** sformułowane przez organizację Childnet (<http://www.childnet.com/>).

- **Strzeż** swojego bezpieczeństwa. Pamiętaj, aby nie ujawniać w Internecie prywatnych danych — takich jak imię, nazwisko, adres e-mail, numer telefonu, adres zamieszkania czy nazwa szkoły — osobom, których nie znasz lub którym nie ufasz.

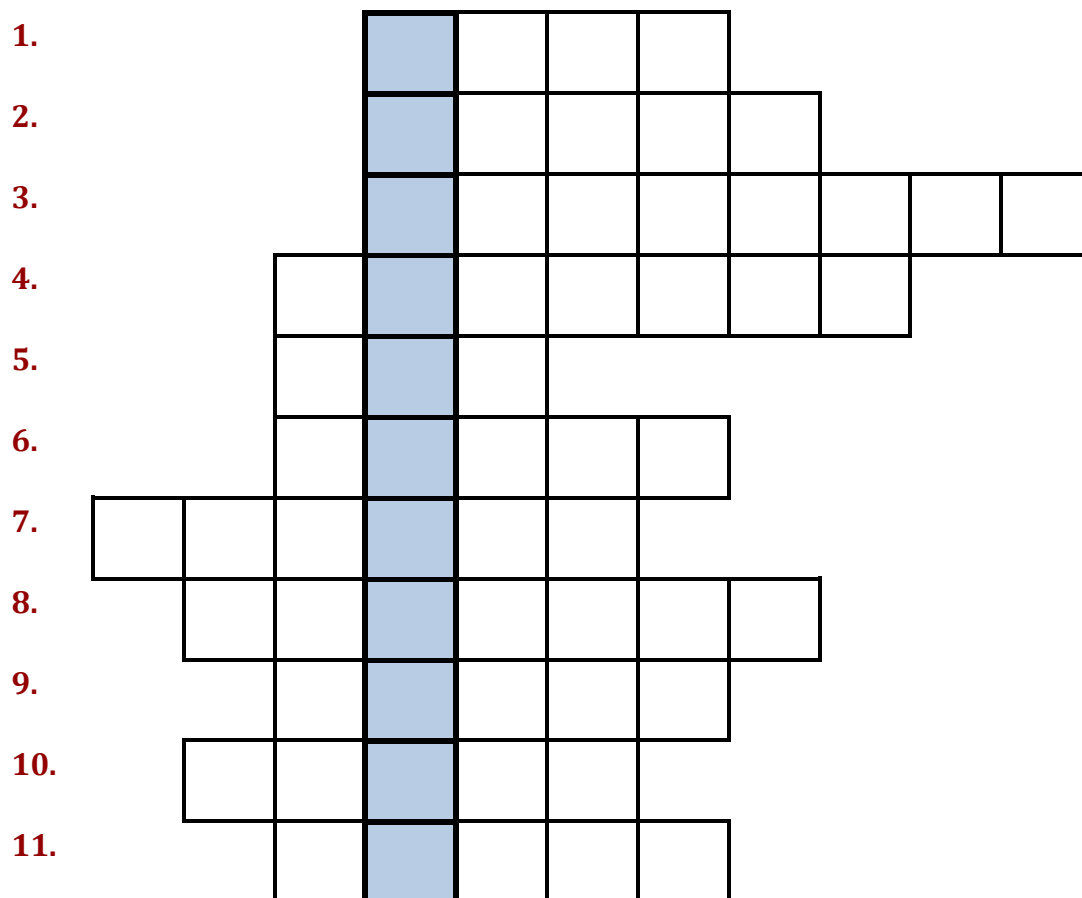
- **Możliwość** spotkania się z kimś, kogo znasz jedynie z sieci, niesie ze sobą niebezpieczeństwo. Rób to jedynie za pozwoleniem rodziców lub opiekunów i wyłącznie w ich obecności.

- **Akceptowanie** wiadomości poczty elektronicznej lub komunikatorów internetowych czy otwieranie plików, obrazów lub tekstu pochodzącego od osób, których nie znasz lub do których nie masz zaufania, może być źródłem problemów — takie dane mogą bowiem zawierać wirusy lub niepokojące informacje.

- **Rozwaga.** Osoby poznane w sieci mogą być w rzeczywistości kimś zupełnie innym, a informacje znalezione w Internecie mogą nie być wiarygodne.

- **To ważne,** aby poinformować rodziców, opiekunów lub zaufaną osobę dorosłą, jeśli ktoś lub coś Cię zaniepokoi, przestraszy lub zawstydzi. Nadużycia internetowe można zgłaszać na policji lub pod adresem **www.dyzurnet.pl**

Rozwiązanie krzyżówki stanowi temat tego artykułu



Hasła do krzyżówki

1. np. 12 maja 2016 roku
2. 02-026 Warszawa, ul. Raszyńska 8/10
3. Nowak, Kowalska
4. 501 123 654 – taki numer ma ...
5. **44 – 113** Gliwice
6. np. pani, dziecko, pan
7. Kasia, Tomek, Ola
8. nie mężczyzna
9. osobisty lub wpłaty
10. fryzjerka, górnik, nauczyciel
11. numer identyfikacyjny

Na podstawie: scenariusza zajęć dla uczniów edukacji wczesnoszkolnej

Temat: Moje dane – moja sprawa.
Chrońmy swoje dane osobowe

Autorki: Bożena Paprocka, Ewa Tarkota
Szkoła Podstawowa nr 38 w Gliwicach

DEKALOG CYFROWEGO OBYWATELA

PRAWA W INTERNECIE

1. Mam prawo czuć się bezpiecznie w sieci.
2. Mam prawo do współtworzenia Internetu.
3. Mam prawo do wyrażania w sieci własnych poglądów i opinii.
4. Mam prawo do ochrony własnego wizerunku w Internecie.
5. Moje dane podlegają ochronie danych osobowych.
6. Mam prawo do korzystania z rzetelnych źródeł informacji.
7. Mogę pobierać programy z otwartą licencją, słuchać udostępnionej muzyki, oglądać legalne filmy.
8. Mam prawo do poszerzania swojej wiedzy poprzez korzystanie z gier edukacyjnych, portali tematycznych i kursów online.
9. Mam prawo do rozrywki w sieci.
10. Mam prawo do komunikowania się z innymi Internautami.

OBOWIĄZKI W INTERNECIE

1. Szanuję innych użytkowników Internetu i traktuję ich tak, jak chcę, żeby oni traktowali mnie.
2. Przestrzegam praw autorskich.
3. Nie używam Internetu, aby szkodzić innym.
4. Korzystam z Internetu z rozwagą i ostrożnością.
5. Mam obowiązek stosowania zasady ograniczonego zaufania wobec ludzi poznanych w sieci oraz informacji w niej znalezionych.
6. Nie używam Internetu, aby kraść.
7. Nie używam Internetu do oszukiwania, nie wprowadzam innych w błąd, dbam, żeby w Internecie było jak najwięcej prawdziwych informacji.
8. Mam obowiązek zachowania kultury w swoich wypowiedziach w sieci.
9. Mam obowiązek brać odpowiedzialność za swoje działania w Internecie.
10. Mam obowiązek informować dorosłych o tym, co mnie zaniepokoi w Internecie.

moje prawa
i obowiązki



DZIEŃ
BEZPIECZNEGO
INTERNETU 2013
www.dzieńpi.pl

NASK



s@ferinternet.pl



Główny
Partner

Fundacja
Orange



Złoty Sponsor
Dzień Bezpiecznego
Internetu 2013



DLACZEGO NALEŻY CHRONIĆ NASZE DANE OSOBOWE?

Żyjemy w dobie przetwarzania danych czyli inaczej mówiąc gromadzenia przekazywania i udostępniania informacji. Wciąż rozsiewamy wokół siebie nasze dane osobowe – w sklepach internetowych podajemy adres do dostawy, zapisujemy swoje e-maile do newsletterów i wrzucamy nasze zdjęcia na różne portale.

Dziś nie ma nowoczesnych usług bez danych osobowych:

- Płacisz kartą kredytową – bank wie, co i jak często kupujesz,
- Rozmawiasz przez komórkę – serwery rejestrują, z kim, jak długo i z jakiego miejsca,
- Wysyłasz maile – już z adresu można czasem poznać, kim jesteś i gdzie pracujesz,
- Kupujesz książkę w sieci – sklep wie, co Ciebie interesuje,
- Serwis społecznościowy zapisuje listę Twoich znajomych,
- Komentujesz i „lajkujesz” – ujawniasz swoje poglądy i pasje,
- Rezerwujesz bilety lotnicze – Twój komputer zostawia wiadomość o tym, jakiego jest typu, jakim programem się posługujesz, jakie są w nim ustawienia.

Dane gromadzi wiele instytucji. Wśród nich są urzędy publiczne, między innymi ZUS, urzędy skarbowe oraz placówki opieki zdrowotnej. Wielokrotnie jesteśmy w nich pytani o nazwisko, adres i numer PESEL. Te dane są potrzebne do ważnej dokumentacji związanej np. z podatkami, prawem jazdy czy naszym leczeniem.

Czy zadawałeś sobie pytanie:

Co się dzieje z danymi o mnie? Co można z nich wywnioskować, kiedy się je zestawia? Kto je analizuje? Po co? Czy instytucje, które gromadzą te dane zabezpieczają je odpowiednio przed wykorzystaniem przez osoby niepowołane?

Co jakiś czas do opinii publicznej trafiają historie o kredytach zaciągniętych na rachunek osób, które nie miały o tym żadnego pojęcia. Można zapytać jak to możliwe. A właśnie możliwe i to często na własne życzenie poszkodowanych.

Po prostu nie chronimy swoich danych osobowych. Podajemy je nieznanym przez telefon.

I potem okazuje się, że mamy kłopoty.

Aby chronić swoje dane, warto przestrzegać kilku wskazówek:

- **Po pierwsze, nigdy nie podawaj osobie nieznajomej numeru pesel przez telefon ani maila.**

- **Po drugie, zrezygnuj z udziału w telefonicznych loteriach, które zapewniają cię o pewnej już wygranej, mimo że nie grałeś.**

- **Po trzecie, nie wysyłaj skanów dowodu osobistego ani prawa jazdy.**

Dla swojego komfortu i bezpieczeństwa, warto chronić informacje o sobie, aby nie zostały użyte w niepożądanym przez nas celu i bez naszej wiedzy.

PSEUDONIMIZACJA – NOWE POJĘCIE

Termin ten zdefiniowany został w RODO (art. 4 ust. 5, motyw 28 i 29 preambuły). Oznacza przetworzenie danych osobowych w taki sposób, by nie można było ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że informacje są przechowywane osobno i objęte są środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej osobie.

Pseudonimizacja danych osobowych oznacza więc **pozbawienie informacji cech danych osobowych**, a zatem możliwości identyfikacji na ich podstawie osoby fizycznej. Jest to proces odwracalny.

Przykłady: Kodowanie prac egzaminu maturalnego, kodowanie prac klasowych

PODSUMOWUJĄC

W dobie facebooka, telefonów rozpoznających twarze, kilkunastu rachunków/rat miesięcznie nasze dane osobowe jak nigdy wcześniej narażone są na „wypłynięcie”. A co może zrobić z nimi oszust? Co tylko chce – kupić telefon, wykorzystać do głosowania czy nawet popełnienia przestępstwa. Wniosek płynący z Europejskiego Dnia Ochrony Danych Osobowych jest więc jasny – chroń swoje dane, to unikniesz kłopotów.

Dane o ... danych

Zgodnie z artykułem 6 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Ochrona danych osobowych to natomiast regulacje prawne dotyczące tworzenia i posługiwania się zbiorami danych osobowych, a także pojedynczymi danymi. Jej celem jest administracyjno-prawna ochrona prawa do prywatności. W Polsce do 2018r. zajmował się tym Generalny Inspektor Ochrony Danych Osobowych (GIODO), powoływany przez Sejm za zgodą Senatu. Obecnie to stanowisko przejął Prezes Urzędu Ochrony Danych Osobowych. Jego kadencja trwa cztery lata. Do Urzędu Ochrony Danych Osobowych (UODO) można zgłaszać wszelkie naruszenia kwestii ochrony danych osobowych.

Co warto wiedzieć – pojęcie ochrony danych nie odnosi się wyłącznie do numeru Pesel, adresu zamieszkania, PINU do karty bankowej czy hasła do poczty e-mail. To także informacje o naszym pochodzeniu, poglądach politycznych, stanie zdrowia czy orientacji seksualnej.



To sygnał dla wszystkich, którzy na facebooku zdradzają zbyt wiele informacji – w ten sposób swoje dane osobowe podają wręcz na tacy. Dobrym przykładem mogą być np. ludzie, którzy udostępniają zdjęcie z wakacji i aktualnym miejscem pobytu. Dla włamywacza to świetna informacja, że domownicy nie zaskoczą go podczas akcji. To skrajny przykład, ale wiele naszych danych zbierają firmy marketingowe, które nie tylko przetwarzają je bez naszej zgody, ale i nimi handlują. Korzystają nie tylko z social media, bowiem w Internecie w dobie tworzenia profili osobowych, masowego korzystania z aplikacji mobilnych, jesteśmy wyjątkowo narażeni na utratę tożsamości. Używamy go do szeregu różnych czynności - płacimy rachunki, robimy zakupy, rozmawiamy ze znajomymi w innych krajach, sprawdzamy natężenie ruchu w danym miejscu, informacje o korkach ulicznych, korzystając z map. Niemal za każdym razem podajemy o sobie wiele informacji, wpisujemy hasła, imię, nazwisko itp.

Chroń swoje dane!

W prawdziwym świecie:

- Nigdy nie pożyczaj nikomu dokumentu, ani nie podawaj danych obcej osobie.
- Nie zostawiaj dowodu osobistego bez nadzoru, np. w wypożyczalni sprzętu.
- Kopie dokumentu tożsamości przekazuj wyłącznie zaufanym instytucjom, i tylko w uzasadnionych przypadkach.
- Jeśli zgubiłeś dowód osobisty albo kartę do bankomatu, natychmiast powiadom o tym stosowny podmiot, np. policję albo bank. Nie chcesz chyba, by ktoś robił zakupy na twój koszt?

W Internecie:

- Nie zostawiaj swoich danych osobowych na cudzym komputerze, np. w urzędzie, bibliotece czy u znajomego. Musisz działać niczym włamywacz i zatrzeć ślady, a więc wyczyścić historię i wylogować się z konta pocztowego, facebooka, bankowości elektronicznej.
- Nie otwieraj nieznanych plików wysłanych na twoją pocztę i nie reaguj na wiadomości bez danych osobowych. Mogą zawierać wirusy, złośliwe oprogramowanie. Niestety, SPAMY są coraz

inteligentniejsze, do tego stopnia, że niekiedy nawet doświadczonym użytkownikom Internetu trudno je odróżnić od normalnego maila. Warto wtedy zwrócić uwagę na adres skrzynki pocztowej z jakiej została wysłana, temat i załączniki. Nawet jeśli przez przypadek otworzymy SPAM pod żadnym pozorem nie wolno podawać swojego numeru telefonu czy innych danych.

- Wygrałeś nowego laptopa, 100 000 zł, wycieczkę na Karaiby albo Mercedesa prosto z salonu? Wygrałeś, choć nie przypominasz sobie udziału w loterii? Niestety, ludzie nadal się na to nabierają, np. starsi. Uświadamiajmy ich, że to fałszywa wiadomość.

- Korzystaj z programów antywirusowych i blokujących złośliwe oprogramowanie. Trzeba tylko pamiętać, że sama instalacja to pół sukcesu, należy jeszcze umiejętnie korzystać z posiadanych narzędzi. A więc przeskanować komputer, dokonywać regularnych aktualizacji oprogramowania.