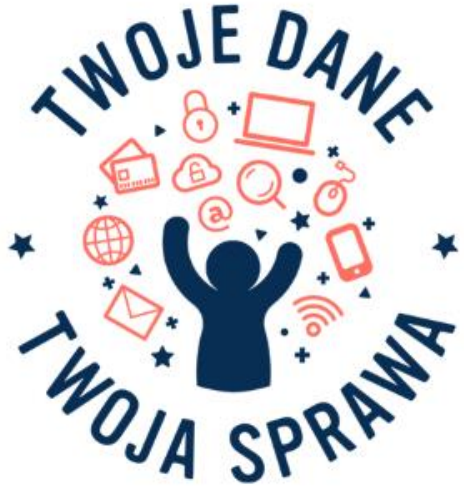


Bezpieczeństwo cyfrowe dzieci i młodzieży a odpowiedzialność

Marta Mikołajczyk, Urząd Ochrony Danych Osobowych
podinsp. Marcin Zimoń, Komenda Stołeczna Policji

URZĄD OCHRONY DANYCH OSOBOWYCH

O czym opowiemy…

Jak odpowiedzialnie i świadomie korzystać
z dostępnych narzędzi w celu ochrony siebie,
swojego wizerunku i danych osobowych,
a także jakie mogą być konsekwencje
nierozważnych decyzji w cyfrowej rzeczywistości.

RODO

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.

Zgodnie z art. 8 RODO dziecko, które ukończyło **16 lat**, może **samodzielnie wyrazić zgodę na przetwarzanie swoich danych,** korzystając tzw. usług społeczeństwa informacyjnego.

Świat nowych technologii ma realny wpływ na nawyki młodych ludzi we wszystkich aspektach życia. Bycie online to nie tylko nasze dane, ale nasze życie nad którym powinniśmy mieć kontrolę.

OGÓLNOPOLSKI PROGRAM EDUKACYJNY PREZESA UODO

Celem programu jest podnoszenie świadomości, informowanie i upowszechnianie wiedzy wśród uczniów i nauczycieli oraz kształtowanie świadomych i odpowiedzialnych postaw w obszarze ochrony danych osobowych.

Patronat honorowy:

MINISTER EDUKACJI NARODOWEJ

Rzecznik Praw Dziecka Mikołaj Pawlak

Partner wpierający:

OEiiZK
Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

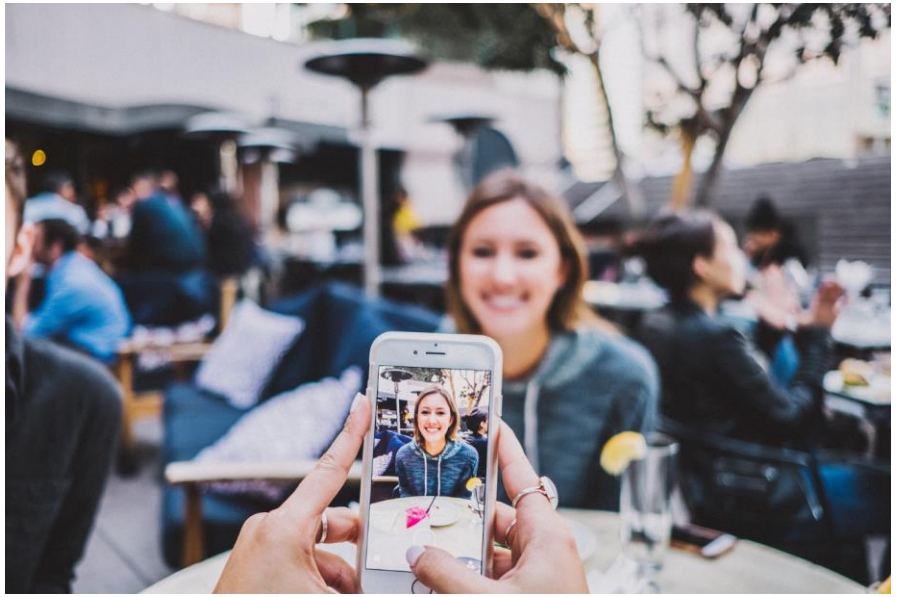
Patroni medialni:

TVP abc, Polskie Radio dzieciom, Rzeczpospolita, Dyrektor Szkoły, Prawo.pl, głosnauczycielski, PortalOświatowy.pl, Ochrona Danych Osobowych, PoradyODO.pl, TIK w edukacji

PRYWATNOŚĆ I DANE OSOBOWE

Dane osobowe to część naszej prywatności.
Dane osobowe to każda informacja umożliwiająca identyfikację konkretnej osoby.
np. imię nazwisko, PESEL, adres, data urodzenia, głos, wizerunek,
Dane szczególnie chronione np. odcisk palca, informacja o nałogach czy zdrowiu.
Zgodnie z prawem wszystkie dane osobowe zasługują na ochronę.

WIZERUNEK TO WAŻNA INFORMACJA O NAS



- **Wizerunek każdego człowieka jest traktowany jako dana osobowa, gdyż daje podstawę ustalenia tożsamości osoby**.

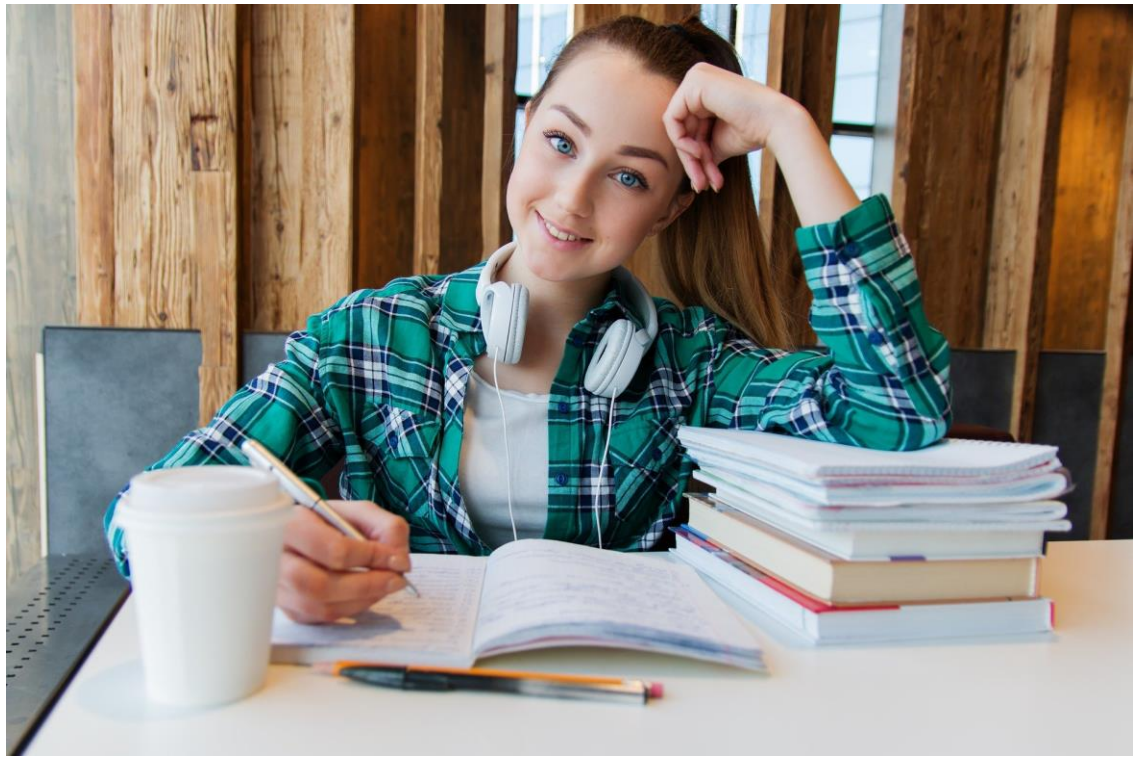
- **Rozpowszechnianie wizerunku danej osoby wymaga jej ZGODY (**z pewnymi wyjątkami).

Zanim wrzucisz do sieci wizerunek innej osoby zastanów się,
czy działasz zgodnie z prawem.

ZGODA NA WYKORZYSTANIE WIZERUNKU UCZNIA W SZKOLE

Szkoła jako administrator danych również przetwarza wizerunek ucznia.

Najczęściej potrzebna jest wtedy **zgoda opiekuna prawnego/rodzica** na jego wykorzystanie np. publikacji wizerunku ucznia np. na stronie szkoły.

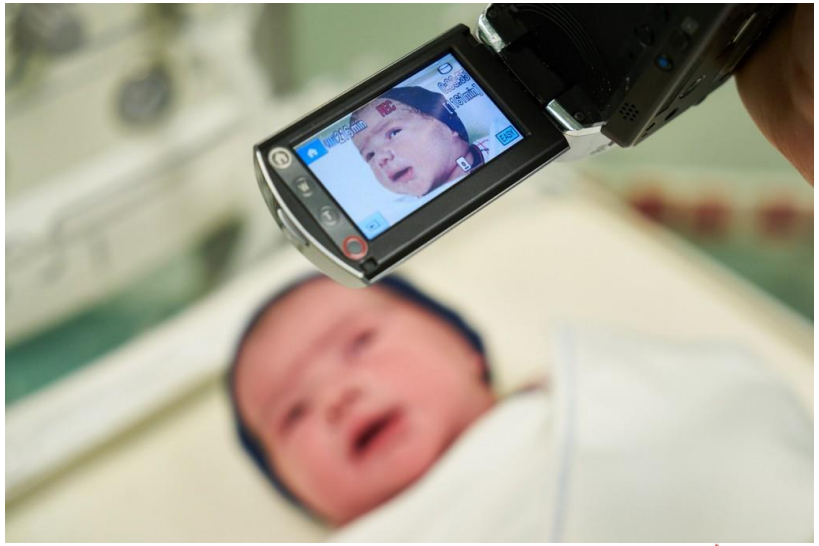


CZY MOŻEMY NAGRYWAĆ LEKCJE ZDALNE?

- Co do zasady, nie powinno się nagrywać lekcji online. Tylko w uzasadnionych przypadkach celami nagrania i przy spełnieniu szeregu warunków, nagranie może być jednak dopuszczalne.
- Włączenie kamer/mikrofonu nie powinno być obowiązkiem na cały czas trwania zajęć.
- Upublicznianie nagrań z lekcji zdalnych w Internecie jest niedopuszczalne i może stanowić naruszenie ochrony danych osobowych.

ZACHWYCASZ SIĘ SWOIMI DZIEĆMI?
ŚWIETNIE, ALE ICH ZDJĘCIA ZOSTAW DLA SIEBIE

- Dużą rolę w ochronie prywatności dziecka w sieci odgrywa świadomy rodzic.
- Przypadków, kiedy rodzice **naruszają prywatność swoich dzieci w Internecie** jest mnóstwo. Niektóre sprawy znalazły swój finał już w sądzie.
- Unikajmy nadmiernego udostępniania zdjęć w Internecie, szczególnie kompromitujących czy zawierających dokumenty np. świadectwa szkolne.



JAK MOŻESZ WSPIERAĆ MŁODYCH LUDZI W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W SIECI?

- **Poszerzaj wiedzę o ochronie danych osobowych** w trosce o bezpieczeństwo swojej rodziny.
- Podejmuj **świadome decyzje w sieci** w obszarze ochrony danych i poszanowania prywatności.
- **Ograniczaj liczbę udostępnianych informacji** o sobie i swoich bliskich w Internecie.
- **Ucz ostrożności** przy podawaniu swoich danych osobowych.
- **Czytaj klauzule informacyjne i zasady ochrony prywatności,** aby wiedzieć jak Twoje dane są przetwarzane.
- **Korzystaj z restrykcyjnych ustawień prywatności**, aby ograniczyć swoją widoczność w sieci.
- Rozmawiaj o ochronie danych osobowych, zagrożeniach i **wspieraj młodych ludzi.**

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

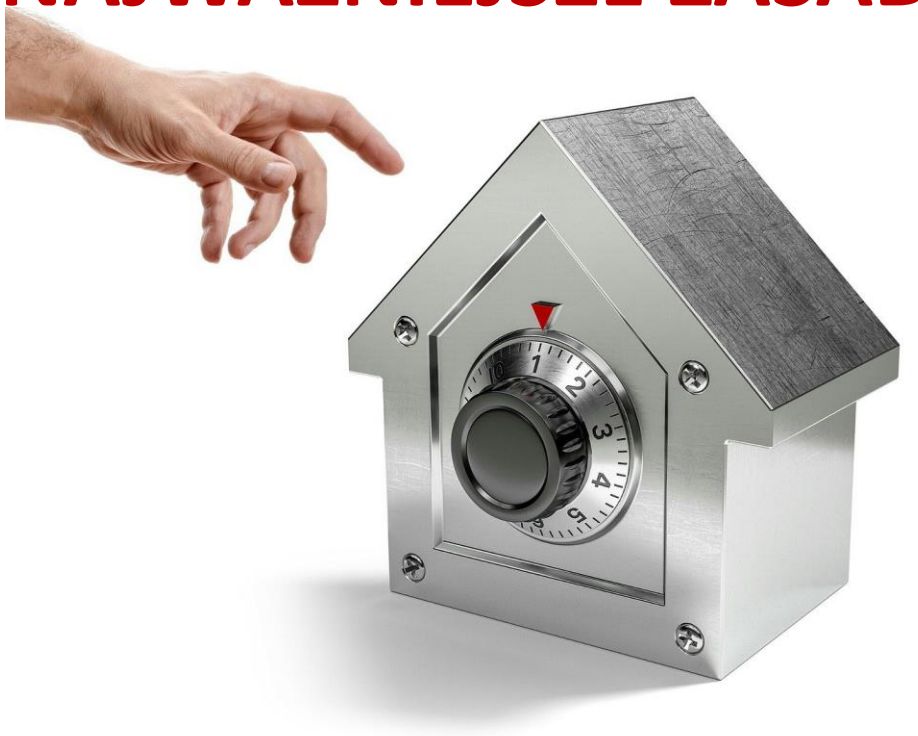
JAK ZAPEWNIĆ SOBIE BEZPIECZEŃSTWO W CYFROWYM ŚWIECIE I ZWIĘKSZYĆ KONTROLĘ NAD SWOIMI DANYMI W SIECI?

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, WIĘC WARTO PAMIĘTAĆ?
JAK CHRONIĆ SWOJE DANE?

NAJWAŻNIEJSZE ZASADY BEZPIECZEŃSTWA:



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

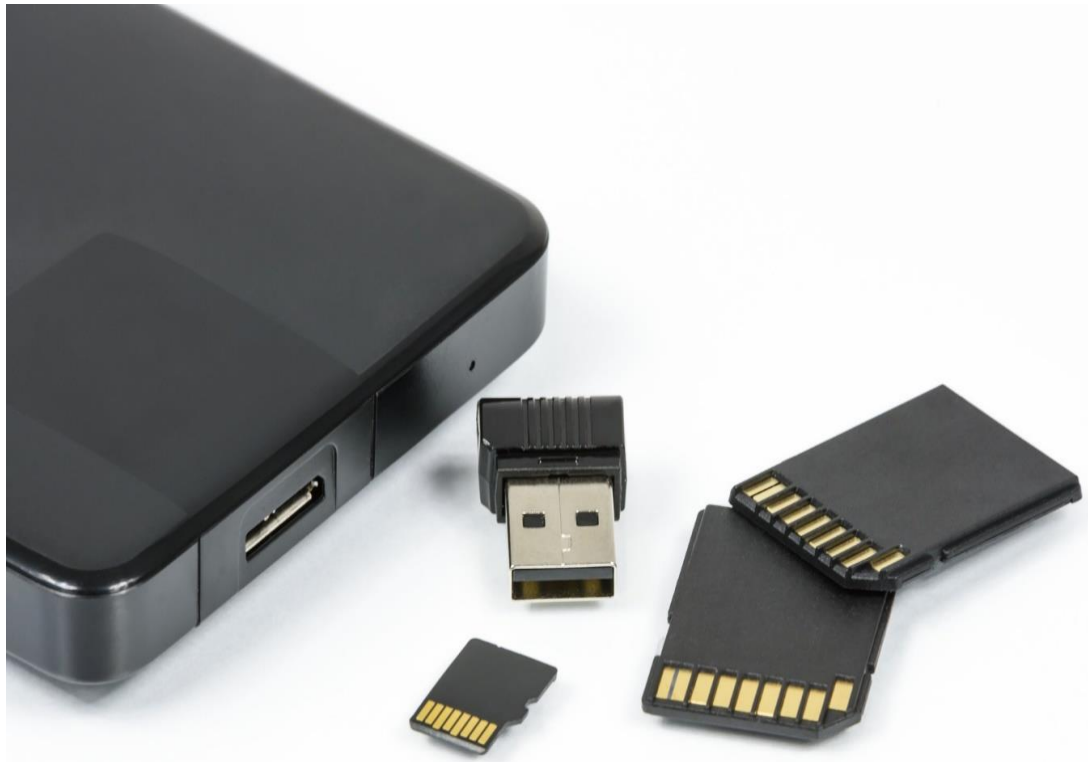
- Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Pamiętaj, że administrator danych musi spełnić wobec Ciebie **obowiązek informacyjny**, czyli przekazać Ci informacje na swój temat tak, abyś miał pewność, przez kogo i w jakim celu dane będą przetwarzane.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

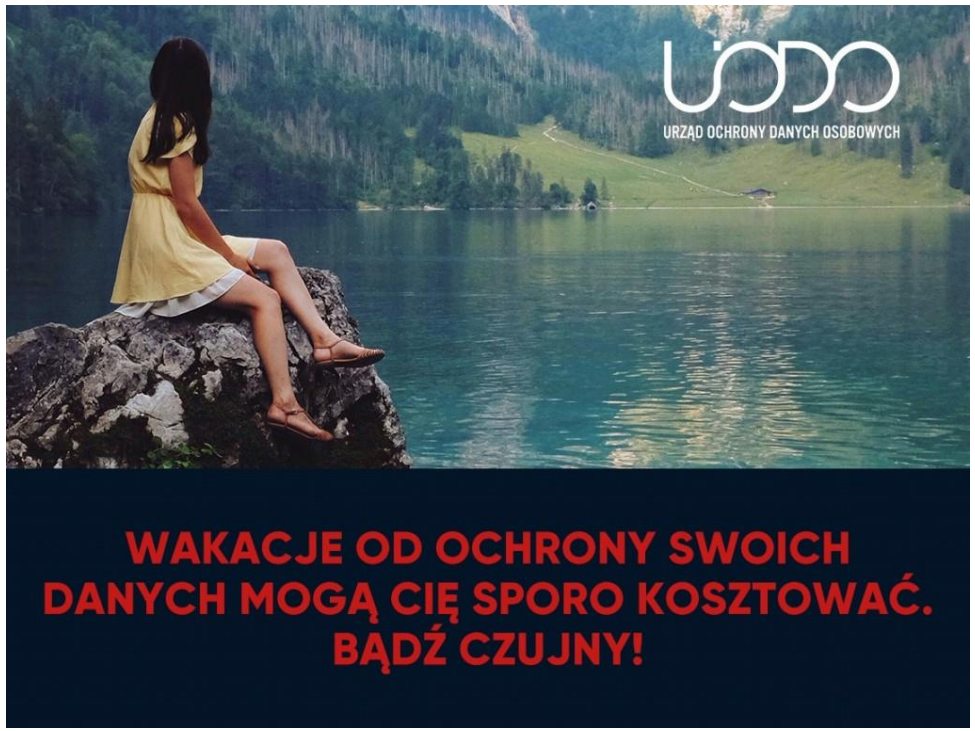
OSTROŻNIE INSTALUJ POTRZEBNE APLIKACJE Z ZAUFANYCH ŹRÓDEŁ

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.



Zadbajmy o swoją prywatność, godność i dane osobowe.

Nie wystarczy sama nasza świadomość ryzyka, ale nasza odpowiedzialność za nie.

DODATKOWE MATERIAŁY

WWW.UODO.GOV.PL

- Chroń swoje dane (https://uodo.gov.pl/pl/138/1267)
- 5 wskazówek, jak bezpiecznie korzystać z aplikacji mobilnych

(https://uodo.gov.pl/pl/138/1122)

- Wakacje od ochrony danych mogą Cię sporo kosztować. Bądź czujny! (https://uodo.gov.pl/pl/138/1575)
- Jak chronić swoje dane osobowe? (https://uodo.gov.pl/pl/138/1221)
- Nie szastaj zdjęciami (https://uodo.gov.pl/pl/18/118)
- Wizerunek dziecka https://uodo.gov.pl/pl/138/1268

DODATKOWE MATERIAŁY

WWW.UODO.GOV.PL

- Darmowe aplikacje. Czy naprawdę są darmowe? (https://uodo.gov.pl/pl/138/1576)
- Warto wiedzieć, jak minimalizować ryzyko kradzieży tożsamości (https://uodo.gov.pl/pl/138/1267)
- Szkoła uczy się chronić dane https://uodo.gov.pl/pl/384/742
- Zadbaj, by twój telefon był przyjacielem, a nie szpiegiem (https://uodo.gov.pl/pl/18/353)
- UODO przypomina jak się zabezpieczyć, gdy wiesz, że wyciekły Twoje dane (https://uodo.gov.pl/pl/138/1300)
- Dane osobowe bezpieczne podczas zdalnego nauczania (https://uodo.gov.pl/pl/138/1473)

Zapraszam na drugą część wykładu