



Temat 4 .

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl>

Ochrona prywatności
i danych osobowych
w cyberprzestrzeni

BEZPIECZEŃSTWO
INFORMACJI



- Prywatność
- Ochrona danych osobowych
- Prywatność w Internecie
- Techniki śledzenia użytkowników
- Przeciwdziałanie śledzeniu użytkowników
- Wirtualna tożsamość
- Regulacje prawne
- Ochrony danych osobowych w organizacji
- Informacje niejawne

Zadanie

Treść

Prezentacja zadania podczas zajęć.

Okolo 9 osób podczas zajęć

(0-2 pkt)



Prywatność

Prywatność

to prawo jednostki do kontrolowania dostępu do swoich **danych osobowych**, informacji oraz aspektów życia osobistego i zawodowego.

Oznacza możliwość decydowania, które informacje zostaną ujawnione, komu i w jakim zakresie, a także ochronę przed nieuprawnionym wglądem, gromadzeniem, przetwarzaniem oraz wykorzystywaniem danych przez osoby trzecie.

W kontekście cyberprzestrzeni

prywatność oznacza ochronę danych osobowych i aktywności użytkownika w sieci przed nieautoryzowanym dostępem, śledzeniem, zbieraniem informacji i manipulacją.

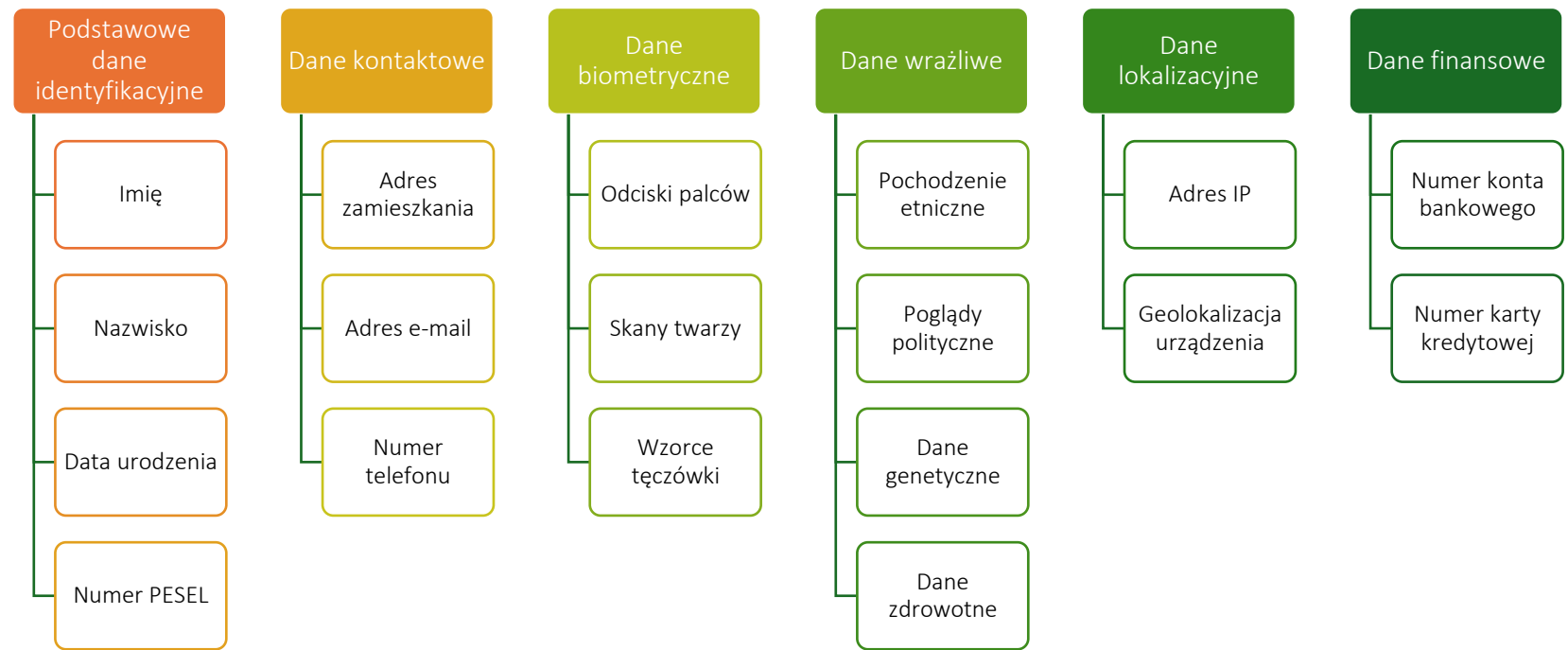


Prywatność

Dane osobowe

to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (tzw. **osoby, której dane dotyczą**).

Możliwość identyfikacji oznacza, że na podstawie tych danych można bezpośrednio lub pośrednio ustalić tożsamość danej osoby.



Ochrona danych osobowych

Ochrona danych osobowych

to zbiór działań i środków podejmowanych w celu zabezpieczenia **danych osobowych** przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, utratą lub zniszczeniem.

Celem ochrony danych jest zapewnienie ich poufności, integralności oraz dostępności, a także przestrzeganie obowiązujących przepisów prawnych dotyczących przetwarzania danych osobowych.

Aspekty techniczne

- to środki i rozwiązania technologiczne mające na celu zabezpieczenie danych przed nieuprawnionym dostępem, modyfikacją lub utratą.

Aspekty organizacyjne

- to procedury, polityki i działania zarządzające przetwarzaniem danych w organizacji, mające na celu zapewnienie zgodności z przepisami oraz minimalizację ryzyka naruszeń.

Ochrona danych osobowych

Kluczowe aspekty ochrony danych

Poufność (Confidentiality):

- Gwarantowanie, że dane są dostępne tylko dla uprawnionych osób.
- Stosowanie mechanizmów takich jak szyfrowanie, uwierzytelnianie użytkowników.

Integralność (Integrity):

- Utrzymanie dokładności i kompletności danych.
- Zabezpieczenie przed nieuprawnioną modyfikacją.

Dostępność (Availability):

- Zapewnienie, że dane są dostępne zawsze, gdy są potrzebne.
- Ochrona przed atakami typu DoS oraz awariami systemów.

Autentyczność (Authenticity):

- Potwierdzenie tożsamości użytkowników i źródeł danych.
- Użycie podpisów cyfrowych i certyfikatów.

Nienaruszalność (Non-repudiation):

- Gwarancja, że osoby przetwarzające dane nie będą mogły zaprzeczyć swoim działaniom.
- Rejestracja operacji w systemie (logowanie).

Ochrona danych osobowych

Aspekty techniczne ochrony danych

Szyfrowanie:

- Kodowanie danych w celu zabezpieczenia ich przed nieuprawnionym dostępem.

Kontrola dostępu:

- Ograniczenie możliwości dostępu do danych wyłącznie dla uprawnionych użytkowników.

Backup danych:

- Tworzenie kopii zapasowych w celu zabezpieczenia przed utratą danych.

Zapory sieciowe (firewalle):

- Filtracja ruchu sieciowego w celu ochrony przed atakami zewnętrznymi.

Systemy wykrywania włamań (IDS):

- Monitorowanie sieci w celu wykrywania nieautoryzowanych działań.

Ochrona danych osobowych

Aspekty organizacyjne ochrony danych

Polityka bezpieczeństwa:

- Zestaw zasad regulujących ochronę danych w organizacji.

Szkolenia pracowników:

- Edukacja na temat bezpiecznego przetwarzania danych osobowych.

Procedury reagowania na incydenty:

- Gotowe plany działania w przypadku naruszenia bezpieczeństwa.

Audyt bezpieczeństwa:

- Regularna weryfikacja systemów i procedur pod kątem zgodności z regulacjami.

Zarządzanie uprawnieniami:

- Określenie zakresu dostępu do danych w zależności od roli w organizacji.

Prywatność w Internecie

Anonimizacja danych

to proces przekształcania danych osobowych w taki sposób, aby niemożliwe było zidentyfikowanie osoby, której dotyczą.

Po anonimizacji dane tracą charakter danych osobowych i nie podlegają przepisom ochrony danych (np. RODO).

Usunięcie wszystkich identyfikujących informacji z bazy danych, takich jak imię, nazwisko, numer PESEL

Przekształcenie danych w sposób nieodwracalny, np. poprzez agregację statystyczną (dane zbiorcze).

Zastosowanie technik takich jak maskowanie danych, aby uniemożliwić identyfikację jednostki.

Prywatność w Internecie

Pseudonimizacja danych

to proces przekształcania danych osobowych w taki sposób, aby nie można było bezpośrednio przypisać ich do konkretnej osoby bez użycia dodatkowych informacji (np. klucza deszyfrującego).

W przeciwieństwie do anonimizacji, pseudonimizacja jest procesem odwracalnym, jeśli posiadamy odpowiednie informacje.

Zastąpienie imienia i nazwiska unikalnym identyfikatorem, np. numerem ID.

Przechowywanie identyfikatora oddzielnie od danych osobowych w bezpiecznym miejscu.

Stosowanie haszowania lub szyfrowania danych w taki sposób, aby można je było później przywrócić do formy oryginalnej.

Prywatność w Internecie

Różnice między anonimizacją a pseudonimizacją

Kryterium	Anonimizacja	Pseudonimizacja
Nieodwracalność	Anonimizacja jest nieodwracalna – raz przekształcone dane nie mogą zostać przywrócone do pierwotnej formy.	Pseudonimizacja może być odwracalna – możliwe jest przywrócenie danych przy użyciu dodatkowych informacji (np. klucza).
Zakres ochrony	Anonimizacja całkowicie usuwa powiązanie z osobą fizyczną, czyniąc dane nieidentyfikowalnymi.	Pseudonimizacja jedynie utrudnia identyfikację, ale powiązanie z osobą może być przywrócone.
Podstawa prawna	Dane zanonimizowane nie podlegają przepisom RODO, ponieważ nie są uznawane za dane osobowe.	Dane pseudonimizowane nadal są uznawane za dane osobowe i podlegają ochronie zgodnie z RODO.

Techniki śledzenia użytkowników

Techniki śledzenia użytkowników

to metody i narzędzia wykorzystywane w Internecie do monitorowania aktywności użytkowników (osób) oraz gromadzenia informacji na temat ich zachowań, preferencji i tożsamości.

Cele

Personalizacja treści

- Umożliwienie dostosowania zawartości stron internetowych do preferencji i zainteresowań użytkownika.

Reklamy kontekstowe

- Prezentowanie reklam dopasowanych do wcześniejszych wyszukiwań i aktywności w sieci.

Analiza ruchu w sieci

- Monitorowanie liczby odwiedzin, interakcji użytkowników oraz ich zachowań na stronie w celu optymalizacji serwisu.

Identyfikacja użytkowników

- Rozpoznawanie użytkowników powracających na stronę w celu zachowania ustawień i danych sesyjnych.

Inwigilacja obywateli

- Wykorzystywanie danych o aktywności online w celach nadzoru, profilowania politycznego lub kontroli społecznej

Techniki śledzenia użytkowników

Techniki śledzenia użytkowników

Pliki cookie:

- Małe pliki tekstowe zapisywane na urządzeniu użytkownika przez przeglądarkę, umożliwiające identyfikację sesji i preferencji.

Fingerprinting:

- Technika identyfikacji urządzenia na podstawie jego unikalnych cech, takich jak konfiguracja przeglądarki czy rozdzielczość ekranu.

Pixel tracking:

- Niewidoczne obrazy (1x1 px) osadzone na stronie internetowej, które zbierają informacje o interakcjach użytkownika.

Local Storage:

- Przechowywanie danych bezpośrednio w przeglądarce w celu zapisywania ustawień i preferencji użytkownika.

Web Beacons:

- Niewielkie, przezroczyste obrazy lub skrypty umieszczane w e-mailach i na stronach, służące do monitorowania otwarć i aktywności.

Third-party tracking:

- Zbieranie danych przez zewnętrzne podmioty (np. sieci reklamowe) w celu śledzenia użytkowników na wielu stronach internetowych.

Browser cache tracking:

- Wykorzystanie pamięci podręcznej przeglądarki do przechowywania danych identyfikujących użytkownika.

ETags (Entity Tags):

- Znaczniki przeglądarki używane do identyfikacji wersji zasobów, które mogą być wykorzystywane do śledzenia użytkowników nawet po wyczyszczeniu plików cookie.

Techniki śledzenia użytkowników

Pliki cookie

to niewielkie pliki tekstowe zapisywane na urządzeniu użytkownika przez przeglądarkę internetową podczas odwiedzania stron internetowych.

Służą do przechowywania informacji o sesji, preferencjach oraz aktywnościach w witrynie.

Rodzaj

Sesyjne:

- Przechowywane tylko podczas trwania sesji przeglądania; usuwane po zamknięciu przeglądarki.

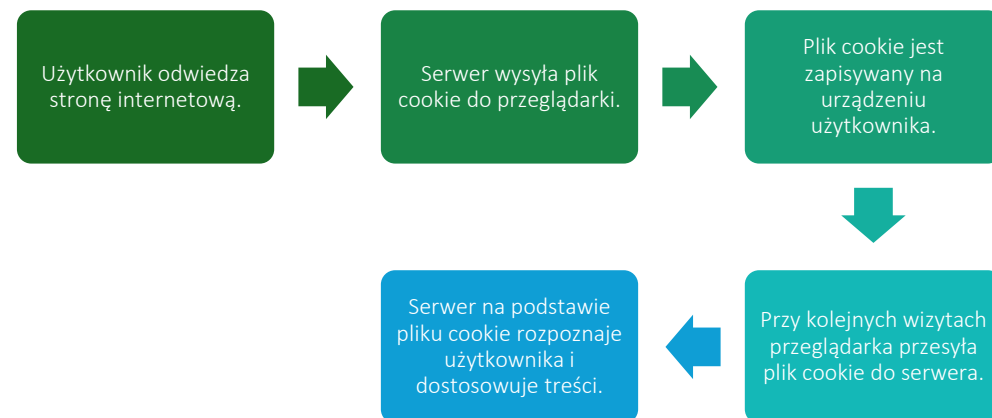
Trwałe:

- Przechowywane na urządzeniu przez określony czas, nawet po zamknięciu przeglądarki.

Śledzące (tracking cookies):

- Stosowane przez strony trzecie do śledzenia aktywności użytkownika na różnych stronach internetowych w celu profilowania reklam.

Mechanizm działania



Techniki śledzenia użytkowników

Fingerprinting

to technika śledzenia użytkowników polegająca na identyfikacji urządzenia na podstawie unikalnych cech przeglądarki i systemu operacyjnego

Cechy

Typ i wersja przeglądarki.

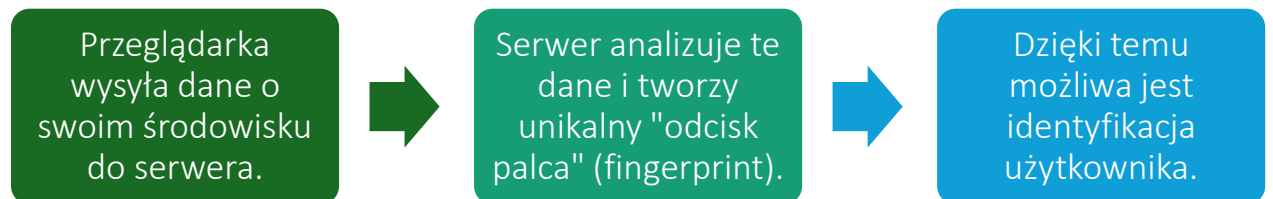
Rozdzielczość ekranu.

Zainstalowane wtyczki i czcionki.

Strefa czasowa i język.

Parametry urządzenia (CPU, GPU).

Mechanizm działania



Techniki śledzenia użytkowników

Pixel tracking

to technika śledzenia użytkowników w Internecie polegająca na umieszczaniu niewidocznych obrazów o wymiarach 1x1 piksel w kodzie stron internetowych lub wiadomości e-mail.

Rodzaj

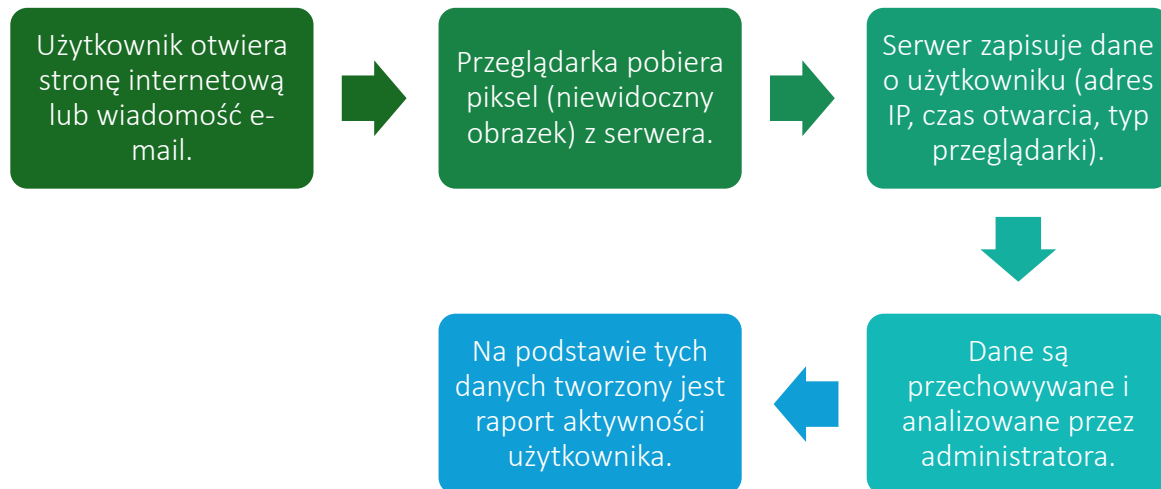
Web tracking pixels:

- Umieszczane na stronach internetowych w celu śledzenia aktywności użytkowników w ramach danej witryny.

Email tracking pixels:

- Osadzone w wiadomościach e-mail do monitorowania otwarć i interakcji z wiadomością.

Mechanizm działania



Przeciwdziałanie śledzeniu użytkowników

Metody przeciwdziałania śledzeniu

to techniki, narzędzia i praktyki mające na celu ochronę prywatności użytkowników w Internecie poprzez blokowanie lub ograniczanie śledzenia ich aktywności przez strony internetowe, reklamy i aplikacje.

Użycie VPN (Virtual Private Network):

- Maskowanie adresu IP oraz szyfrowanie ruchu internetowego w celu zachowania anonimowości.

Przeglądarki wspierające ochronę prywatności:

- Używanie przeglądarek takich jak Tor, Brave czy Firefox z dodatkowymi zabezpieczeniami.

Rozszerzenia blokujące skrypty śledzące:

- Instalacja wtyczek takich jak uBlock Origin, Privacy Badger, Ghostery czy NoScript.

Blokowanie plików cookie:

- Wyłączenie akceptacji plików cookie stron trzecich lub ich automatyczne usuwanie po zakończeniu sesji.

Anonimowe tryby przeglądania:

- Korzystanie z trybu incognito lub prywatnego w przeglądarce.

Blokowanie pikseli śledzących:

- Wykorzystanie dodatków blokujących niewidoczne obrazy (pixel tracking) w e-mailach i na stronach.

Skrypty anty-fingerprint:

- Użycie wtyczek, które zmieniają parametry przeglądarki w celu utrudnienia identyfikacji urządzenia.

Ograniczanie śledzenia w ustawieniach przeglądarki:

- Włączenie funkcji "Do Not Track" oraz blokowanie śledzenia w ustawieniach prywatności.

Przeciwdziałanie śledzeniu użytkowników

Użycie VPN (Virtual Private Network)

to technologia umożliwiająca tworzenie bezpiecznego i szyfrowanego połączenia między urządzeniem użytkownika a serwerem VPN w Internecie. Dzięki temu cały ruch internetowy jest maskowany i chroniony przed nieautoryzowanym dostępem.

Korzyści

Anonimowość:

- Ukrycie rzeczywistego adresu IP i lokalizacji użytkownika.

Bezpieczeństwo:

- Szyfrowanie chroni dane przed przechwyceniem, nawet w przypadku korzystania z niezabezpieczonych sieci Wi-Fi.

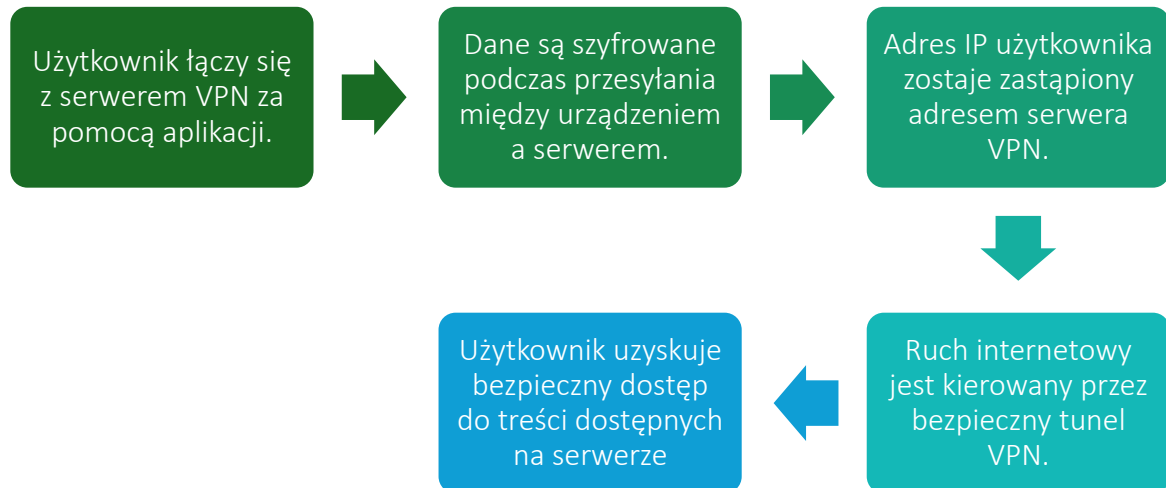
Prywatność:

- Ochrona przed śledzeniem przez dostawców Internetu, strony internetowe i reklamodawców.

Ochrona przed atakami:

- Redukcja ryzyka przechwycenia danych w publicznych hotspotach Wi-Fi.

Mechanizm działania



Przeciwdziałanie śledzeniu użytkowników

Przeglądarki wspierające ochronę prywatności

to specjalne aplikacje internetowe zaprojektowane z myślą o minimalizowaniu śledzenia użytkownika, ochronie danych osobowych oraz zwiększeniu anonimowości podczas przeglądania stron internetowych.

Przeglądarka blokuje pliki cookie stron trzecich.

Przeglądarka blokuje skrypty śledzące.

Przeglądarka chroni przed fingerprintingiem.

Przeglądarka nie zapisuje historii przeglądania.

Przeglądarka automatycznie usuwa ciasteczka po zamknięciu sesji.

Przeglądarka nie rejestruje aktywności użytkownika.

Przeglądarka chroni dane przed śledzeniem.

Przeglądarka ukrywa adres IP użytkownika (np. Tor).

Przeciwdziałanie śledzeniu użytkowników

Przeglądarki wspierające ochronę prywatności

	Nazwa przeglądarki	Opis	Link do pobrania
	Tor Browser	Zapewnia pełną anonimowość poprzez maskowanie adresu IP i szyfrowanie ruchu w sieci Tor.	https://www.torproject.org/
	Brave	Automatycznie blokuje reklamy, śledzenie i pliki cookie stron trzecich.	https://brave.com/
	Firefox (z dodatkami)	Umożliwia instalację rozszerzeń blokujących śledzenie (np. uBlock Origin, Privacy Badger).	https://www.mozilla.org/firefox/
	DuckDuckGo Browser	Chroni prywatność, nie zapisuje historii przeglądania, blokuje trackery.	https://duckduckgo.com/app

Wirtualna tożsamość

Wirtualna tożsamość

to zbiór danych osobowych oraz informacji wykorzystywanych przez użytkownika do reprezentowania siebie w cyberprzestrzeni.

Może obejmować pseudonimy (nick), adresy e-mail, awatary czy profile na portalach społecznościowych.

Wirtualna tożsamość pozwala na interakcję w Internecie bez ujawniania prawdziwej tożsamości użytkownika.

Konta pseudonimowe:

Zakładanie profili z fikcyjnymi imionami lub pseudonimami.

Tymczasowe adresy e-mail:

Wykorzystanie jednorazowych lub aliasowych adresów w celu ochrony prywatności.

Awatary i zdjęcia profilowe:

Używanie grafik zamiast rzeczywistych zdjęć w profilach społecznościowych.

Zmienione dane lokalizacyjne:

Użycie VPN do zmiany widocznego miejsca połączenia.

Konta na forach i w grach:

Tworzenie odrębnych tożsamości dla różnych społeczności internetowych.

Wirtualna tożsamość

Korzyści

Ochrona prywatności:

- Użytkownik nie ujawnia swoich prawdziwych danych osobowych.

Bezpieczeństwo w sieci:

- Zmniejszenie ryzyka ataków typu phishing czy kradzieży tożsamości.

Wolność wypowiedzi:

- Możliwość swobodnego wyrażania opinii bez obawy przed represjami.

Oddzielenie ról społecznych:

- Możliwość utrzymania rozdziału między życiem prywatnym a zawodowym.

Minimalizacja śledzenia:

- Trudniejsze profilowanie użytkownika przez reklamodawców.

Wirtualna tożsamość

Zagrożenia

Cyberprzestępczość:

- Anonimowość może być wykorzystywana do oszustw i nadużyć.

Fałszywe profile:

- Możliwość tworzenia fikcyjnych kont w celu manipulacji i dezinformacji.

Brak odpowiedzialności:

- Trudniejsza identyfikacja osób odpowiedzialnych za hejt czy oszustwa.

Zaufanie w sieci:

- Utrudniona weryfikacja autentyczności tożsamości rozmówców.

Trudności w wykrywaniu przestępstw:

- Organy ścigania napotykają na problemy z identyfikacją osób działających anonimowo.

Regulacje prawne

Regulacje prawne ochrony danych

Obszar	Nazwa aktu prawnego	Opis	Rok	Tekst aktu prawnego
UE	Ogólne Rozporządzenie o Ochronie Danych (RODO)	Rozporządzenie (UE) 2016/679, które reguluje przetwarzanie danych osobowych w UE. Ujednolica przepisy we wszystkich państwach członkowskich, wzmacnia prawa obywateli i obowiązki administratorów danych.	2018 r.	https://eur-lex.europa.eu/eli/reg/2016/679/oj
UE	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680	Dotyczy ochrony danych osobowych przetwarzanych przez organy ścigania w celu zapobiegania przestępczości oraz wykrywania i ścigania czynów zabronionych. Określa zasady przetwarzania danych przez służby porządkowe.	2016 r.	https://eur-lex.europa.eu/eli/dir/2016/680/oj
Polska	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych	Ustawa krajowa dostosowująca polskie przepisy do wymogów RODO. Określa zadania Prezesa Urzędu Ochrony Danych Osobowych (UODO) oraz zasady przetwarzania danych w Polsce.	2018 r.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000
Polska	Konstytucja Rzeczypospolitej Polskiej	Najwyższy akt prawny w Polsce, który gwarantuje prawo do prywatności oraz ochrony danych osobowych jako jedno z podstawowych praw obywatelskich.	1997 r.	https://www.sejm.gov.pl/prawo/konst/polski/kon1.htm
Polska	Kodeks karny - Rozdział XXXIII: Przestępstwa przeciwko ochronie informacji	Reguluje przestępstwa związane z naruszeniem ochrony informacji niejawnych oraz danych osobowych. Dotyczy m.in. ujawniania tajemnic, przetwarzania zabezpieczeń i bezprawnego uzyskania informacji.	1997 r.	https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/roz-33

Regulacje prawne

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)

<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Ujednolica przepisy w zakresie przetwarzania danych we wszystkich państwach członkowskich UE.

Wzmacnia prawa obywateli do ochrony danych osobowych.

Nakłada obowiązki na administratorów danych w zakresie przetwarzania, zabezpieczenia i zgłaszania naruszeń danych.

Zapewnia większą kontrolę użytkowników nad ich danymi.

Wprowadza kary finansowe za naruszenie przepisów.

Regulacje prawne

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

<https://eur-lex.europa.eu/eli/dir/2016/680/oj>

Określa zasady przetwarzania danych przez służby porządkowe w Unii Europejskiej.

Wprowadza przepisy dotyczące bezpieczeństwa danych przetwarzanych przez organy ścigania i wymiany informacji między krajami UE.

Zapewnia równowagę między potrzebą ochrony danych a interesem publicznym związanym z bezpieczeństwem.

Regulacje prawne

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Ustawa krajowa dostosowująca polskie przepisy do wymogów RODO (Rozporządzenie Ogólne o Ochronie Danych).

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000>

Reguluje zasady przetwarzania danych osobowych w Polsce.

Określa zadania i kompetencje Prezesa Urzędu Ochrony Danych Osobowych (UODO).

Wprowadza przepisy dotyczące kontroli przetwarzania danych osobowych oraz sankcji za ich naruszenie.

Dostosowuje krajowe regulacje do europejskich standardów ochrony danych osobowych.

Regulacje prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.

to podstawowy i najwyższy akt prawny w Polsce.

<https://www.sejm.gov.pl/prawo/konst/polski/kon1.htm>

Gwarantuje prawo do prywatności oraz ochrony danych osobowych jako jedno z podstawowych praw obywatelskich.

Stanowi fundament ochrony wolności i praw człowieka oraz obywatela.

Wprowadza zasady przetwarzania danych w kontekście ochrony prywatności, co znajduje odzwierciedlenie w dalszych regulacjach prawnych.

Zapewnia obywatelom ochronę przed bezprawnym pozyskiwaniem, przetwarzaniem i wykorzystywaniem danych osobowych.

Regulacje prawne

Kodeks karny - Rozdział XXXIII: Przestępstwa przeciwko ochronie informacji

reguluje przestępstwa przeciwko ochronie informacji, w tym naruszenia ochrony danych osobowych oraz informacji niejawnych.

<https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/roz-33>

Dotyczy ujawniania tajemnic służbowych, zawodowych oraz innych chronionych prawnie informacji.

Obejmuje przestępstwa związane z bezprawnym uzyskiwaniem danych, przełamywaniem zabezpieczeń oraz sabotażem informatycznym.

Przewiduje kary za bezprawne zdobycie, modyfikację lub zniszczenie danych.

Chroni dane zarówno w kontekście informatycznym, jak i w tradycyjnych formach przechowywania informacji.

Regulacje prawne

Artykuł	Tytuł/Opis	Czego dotyczy
Art. 265	Ujawnienie informacji niejawnych	Ujawnienie lub wykorzystanie informacji niejawnych bez uprawnienia.
Art. 266	Naruszenie tajemnicy służbowej, zawodowej lub innej tajemnicy ustawowej	Naruszenie obowiązku zachowania tajemnicy przez osobę zobowiązaną do jej ochrony.
Art. 267	Bezprawne uzyskanie informacji	Uzyskanie dostępu do informacji nieprzeznaczonej dla danej osoby poprzez przełamanie zabezpieczeń, podsłuch lub inne środki.
Art. 268	Niszczenie, uszkodzanie lub zmiana danych informatycznych	Bezprawne zniszczenie, uszkodzenie, usunięcie lub zmiana zapisanych danych informatycznych.
Art. 268a	Zakłócenie pracy systemu komputerowego	Bezprawne wprowadzenie danych lub ich zmiana w systemie komputerowym, co prowadzi do zakłócenia jego pracy.
Art. 269	Sabotaż informatyczny	Niszczenie danych lub zakłócanie pracy systemu komputerowego w celu wyrządzenia szkody.
Art. 269a	Atak na system komputerowy w celu uzyskania korzyści majątkowej	Zakłócenie systemu komputerowego w celu osiągnięcia korzyści majątkowej lub osobistej.
Art. 269b	Tworzenie, nabywanie lub udostępnianie złośliwego oprogramowania	Produkcja, zakup, sprzedaż lub rozpowszechnianie programów komputerowych przeznaczonych do popełnienia przestępstwa (np. wirusów).
Art. 270	Fałszowanie dokumentów komputerowych	Wytwarzanie, przerabianie lub podrabianie danych komputerowych w celu użycia jako autentyczne.
Art. 271	Poświadczenie nieprawdy w dokumencie elektronicznym	Wystawienie dokumentu elektronicznego przez osobę uprawnioną, który zawiera nieprawdziwe dane, mogące mieć znaczenie prawne.
Art. 272	Podszywanie się pod inną osobę (kradzież tożsamości)	Uzyskanie informacji lub danych osobowych w celu podszycia się pod inną osobę, z użyciem fałszywego dokumentu lub danych osobowych.

Ochrony danych osobowych w organizacji

Urząd Ochrony Danych Osobowych (UODO)

to centralny organ administracji publicznej odpowiedzialny za nadzór nad przestrzeganiem przepisów o ochronie danych osobowych w Polsce.

Kontrola przetwarzania danych osobowych:

- Przeprowadzanie inspekcji w podmiotach przetwarzających dane osobowe.

Wydawanie decyzji administracyjnych:

- Nakładanie kar finansowych za naruszenie przepisów RODO i krajowych ustaw o ochronie danych.

Opiniowanie i edukacja:

- Opracowywanie wytycznych i zaleceń w zakresie ochrony danych.
- Prowadzenie działań edukacyjnych w zakresie przepisów o ochronie danych osobowych.

Rozpatrywanie skarg:

- Przyjmowanie i rozpatrywanie skarg obywateli dotyczących naruszeń ochrony danych.

Współpraca międzynarodowa:

- Wymiana informacji i współpraca z organami ochrony danych w innych krajach Unii Europejskiej.

Powstał na mocy
ustawy z dnia 10 maja 2018r.
o ochronie danych osobowych.

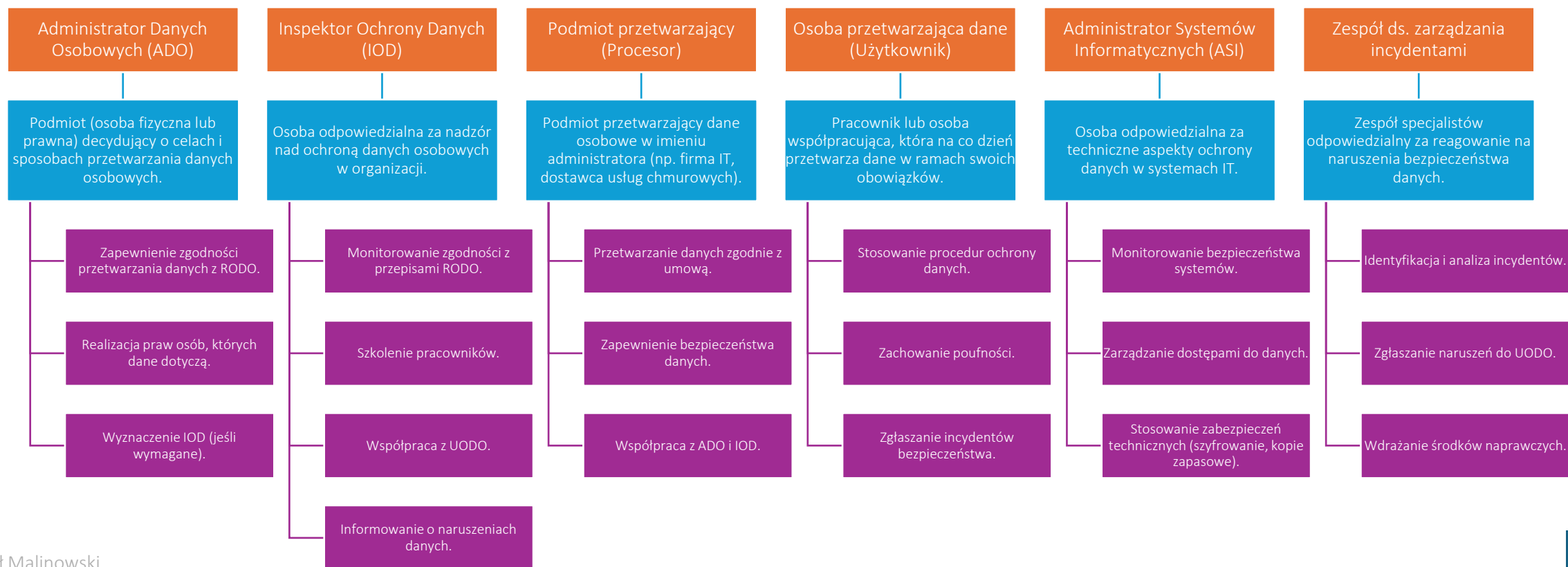
Ochrony danych osobowych w organizacji

Wymogi nakładane na organizacje przez UODO

Wymóg	Opis
Wyznaczenie Inspektora Ochrony Danych (IOD)	Obowiązek powołania IOD w instytucjach publicznych oraz firmach przetwarzających dane na dużą skalę.
Prowadzenie rejestru czynności przetwarzania	Dokumentowanie operacji przetwarzania danych, w tym ich celów i podstaw prawnych.
Zapewnienie zgodności z RODO	Stosowanie zasad ochrony danych osobowych w codziennej działalności (m.in. minimalizacja i rozliczalność).
Realizacja praw osób, których dane dotyczą	Zapewnienie dostępu do danych, prawa do sprostowania, usunięcia oraz przenoszenia danych.
Ocena skutków dla ochrony danych (DPIA)	Obowiązek przeprowadzenia DPIA w przypadku operacji przetwarzania mogących naruszyć prawa osób fizycznych.
Obowiązek zgłaszania naruszeń danych.	Zgłaszanie incydentów bezpieczeństwa danych do UODO w ciągu 72 godzin od ich wykrycia.
Stosowanie odpowiednich zabezpieczeń	Techniczne i organizacyjne środki ochrony danych (m.in. szyfrowanie, pseudonimizacja).
Szkolenie personelu	Edukacja pracowników w zakresie ochrony danych osobowych oraz przetwarzania zgodnego z RODO.
Opracowanie polityki prywatności	Dokument określający zasady przetwarzania danych w organizacji oraz obowiązki administratora danych.

Ochrony danych osobowych w organizacji

Podstawowe role w organizacji w zakresie ochrony danych osobowych



Ochrony danych osobowych w organizacji

Rejestr czynności przetwarzania

to dokument, w którym administrator danych (ADO) zapisuje wszystkie operacje przetwarzania danych osobowych w organizacji.

Jest to kluczowy element dokumentacji ochrony danych wymagany przez RODO.

Przykład

Lp.	Cel przetwarzania	Kategorie danych	Podstawa prawna	Odbiorcy danych	Okres przechowywania
1	Obsługa kadrowa	Imię, nazwisko, PESEL	Umowa o pracę	Dział kadr	10 lat
2	Marketing usług	Adres e-mail, imię	Zgoda	Dział marketingu	Do czasu wycofania zgody
3	Realizacja umowy z klientem	Dane kontaktowe, NIP	Umowa	Dział obsługi klienta	5 lat po zakończeniu umowy

Co powinien zawierać rejestr czynności przetwarzania?

Dane administratora i IOD:

- Nazwa, dane kontaktowe administratora oraz ewentualnie Inspektora Ochrony Danych.

Cele przetwarzania:

- Dlaczego dane są zbierane i w jakim celu są przetwarzane.

Opis kategorii danych osobowych:

- Jakie dane są przetwarzane (np. dane identyfikacyjne, adresowe, finansowe).

Kategorie osób, których dane dotyczą:

- Pracownicy, klienci, kontrahenci, użytkownicy usług.

Podstawa prawna przetwarzania:

- Zgoda, umowa, obowiązek prawny, uzasadniony interes.

Odbiorcy danych osobowych:

- Kto ma dostęp do danych (np. procesorzy, dostawcy usług IT, instytucje publiczne).

Przekazywanie danych do państw trzecich:

- Informacja o transferze danych poza Europejski Obszar Gospodarczy (EOG).

Okres przechowywania danych:

- Jak długo dane będą przechowywane przed ich usunięciem.

Środki techniczne i organizacyjne:

- Zabezpieczenia zastosowane w celu ochrony danych (np. szyfrowanie, pseudonimizacja).

Ochrony danych osobowych w organizacji

Obowiązek zgłaszania naruszeń danych osobowych

Naruszenie ochrony danych osobowych to sytuacja, w której dochodzi do:

- Nieuprawnionego dostępu do danych (np. atak hakerski).
- Utraty danych (np. zgubiony pendrive z danymi osobowymi).
- Usunięcia lub modyfikacji danych bez zgody (np. sabotaż).
- Wycieku danych (np. niekontrolowane udostępnienie danych osobom trzecim).

Przykład

Administrator danych: XYZ Sp. z o.o.

Opis naruszenia: Kradzież laptopa zawierającego dane osobowe klientów.

Kategorie danych: Imię, nazwisko, adres e-mail, numer PESEL.

Liczba osób poszkodowanych: 500

Skutki: Możliwość nieuprawnionego wykorzystania danych osobowych.

Środki zaradcze: Zgłoszenie na policję, zmiana haseł w systemach, powiadomienie osób poszkodowanych.

Kontakt do IOD: Jan Kowalski, iod@xyz.pl

Co powinno zawierać zgłoszenie?

Opis naruszenia:

- Co się wydarzyło? Jak doszło do incydentu?

Kategorie i liczba poszkodowanych osób:

- Ilu osobom dotyczy incydent? Jakie dane zostały naruszone?

Kategorie i liczba rekordów danych:

- Ile rekordów zostało ujawnionych lub utraconych?

Skutki naruszenia:

- Możliwe konsekwencje naruszenia danych osobowych.

Środki zaradcze:

- Jakie kroki podjęto w celu minimalizacji szkód i zapobieżenia dalszym naruszeniom.

Dane kontaktowe IOD:

- Dane osoby odpowiedzialnej za zarządzanie incydentem w organizacji.

Ochrony danych osobowych w organizacji

Podstawa prawna

- Obowiązek zgłaszania naruszeń wynika z RODO (art. 33).
- Zgłoszenie musi być dokonane do Urzędu Ochrony Danych Osobowych (UODO) w ciągu 72 godzin od wykrycia incydentu.

Kto musi zgłaszać naruszenie?

- Administrator Danych Osobowych (ADO) - ponosi główną odpowiedzialność za zgłoszenie naruszenia.
- W przypadku, gdy dane są przetwarzane przez procesora, to on jest zobowiązany do niezwłocznego poinformowania ADO o incydencie.

Skutki braku zgłoszenia:

- **Kara finansowa:** Do 10 milionów EUR lub 2% rocznego obrotu organizacji.
- **Odpowiedzialność cywilna:** Możliwość roszczeń odszkodowawczych od poszkodowanych osób.
- **Uszczerbek na reputacji:** Negatywny wpływ na wizerunek organizacji.

Powiadomienie osób poszkodowanych

Jeśli naruszenie danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi powiadomić te osoby bez zbędnej zwłoki.

Informacje niejawne

Informacji niejawnych

to dane, których nieuprawnione ujawnienie mogłoby spowodować szkodę dla interesów państwa, organizacji lub bezpieczeństwa narodowego.

Ochrona takich informacji polega na stosowaniu środków organizacyjnych, technicznych i prawnych zapobiegających ich ujawnieniu, modyfikacji lub zniszczeniu.

Podstawy prawne

Obszar	Nazwa aktu prawnego	Opis	Rok	Tekst aktu prawnego
Polska	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	Reguluje zasady klasyfikacji i ochrony informacji niejawnych w Polsce.	2011 r.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=W DU20101821228
UE	Decyzja Rady 2013/488/UE	Określa zasady ochrony informacji niejawnych w instytucjach Unii Europejskiej.	2013 r.	https://eur-lex.europa.eu/eli/dec/2013/488/oj
NATO	Polityka ochrony informacji NATO (C-M(2002)49)	Ustanawia standardy ochrony informacji w ramach struktur NATO.	2002 r.	https://bip.abw.gov.pl/download/1/1207/CM_2002_49COR9.pdf

Informacje niejawne

Porównanie kategorii tajności

Kategoria	Polska	Unia Europejska (UE)	NATO	Opis
Najwyższa (Top Secret)	Ścisłe tajne	TRÈS SECRET UE / EU TOP SECRET	COSMIC TOP SECRET (CTS)	Ujawnienie spowoduje wyjątkowo poważną szkodę dla bezpieczeństwa państwa lub organizacji.
Wysoka (Secret)	Tajne	SECRET UE	NATO SECRET (NS)	Ujawnienie spowoduje poważną szkodę dla interesów państwowych, organizacyjnych lub sojuszniczych.
Średnia (Confidential)	Poufne	CONFIDENTIEL UE	NATO CONFIDENTIAL (NC)	Ujawnienie może zaszkodzić interesom organizacji lub państwa, ale bez poważnych skutków.
Niska (Restricted)	Zastrzeżone	RESTREINT UE	NATO RESTRICTED (NR)	Ujawnienie może być niekorzystne , ale nie stanowi bezpośredniego zagrożenia dla bezpieczeństwa.

Informacje niejawne

Dostęp do informacji niejawnych

Dostęp uzyskuje się tylko po:

- pozytywnej weryfikacji bezpieczeństwa osobowego przez ABW/SKW,
- szkoleniu w zakresie ochrony informacji niejawnych,
- podpisaniu oświadczenia o zachowaniu tajemnicy.

Osoby posiadające dostęp muszą przestrzegać zasady „need to know” – dostęp tylko, jeśli jest to niezbędne do wykonywania obowiązków

Kancelarie tajne i systemy ewidencji

Instytucje przetwarzające informacje niejawne prowadzą kancelarie tajne, które:

- przyjmują, przechowują, rejestrują i wydają dokumenty niejawne,
- zapewniają śledzenie obiegu dokumentacji.

Kancelarie mogą być jawne lub niejawne, prowadzone manualnie lub elektronicznie (zgodnie z wymaganiami ABW).

Informacje niejawne

Środki ochrony

Bezpieczne strefy:
wydzielone pomieszczenia lub
strefy o kontrolowanym dostępie
(tzw. strefy bezpieczeństwa).

Systemy ochrony fizycznej:
sejfy, zamki elektroniczne,
systemy alarmowe, ochrona
osobowa.

Zabezpieczenia
teleinformatyczne:

certyfikowane
systemy
kryptograficzne,

kontrola dostępu do
systemów (logowanie,
biometria),

ewidencja dostępu do
plików i nośników.

Zabezpieczenia proceduralne:

instrukcje
kancelaryjne,

procedury nadania,
zmiany i zniesienia
klauzuli tajności,

protokoły
przekazywania
informacji.

Odpowiedzialność karna i dyscyplinarna

Ujawnienie informacji niejawnych może skutkować:

- odpowiedzialnością karną (Kodeks karny, art. 265–269),
- utratą certyfikatu bezpieczeństwa,
- karami dyscyplinarnymi lub wydaleniem z pracy/służby,
- zerwaniem umowy z podmiotem zewnętrznym.

Zadanie

(0-2 pkt)

Treść

Na podstawie obowiązujących aktów prawnych dotyczących ochrony danych osobowych Polsce odpowiedź na poniższe pytania i uzasadnij:

1. Monitoring na osiedlach i przy domofonach
Czy wspólnota może nagrywać mieszkańców i gości bez ich zgody?
2. Publiczne listy obecności i wyniki rekrutacji
Czy można publikować imiona i nazwiska uczestników na tablicy lub stronie?
3. Przekazywanie danych rodziców przez szkoły
Czy szkoła może udostępnić dane rodziców np. radzie rodziców lub ubezpieczycielowi?
4. Używanie prywatnych komunikatorów do kontaktów służbowych
Czy pracownik może pisać do klientów lub uczniów przez Messenger/WhatsApp?

Termin przesłania sprawozdania,
wskazany w zadaniu w Moodle.

