OKRĘGOWA IZBA LEKARSKA W KOSZALINIE

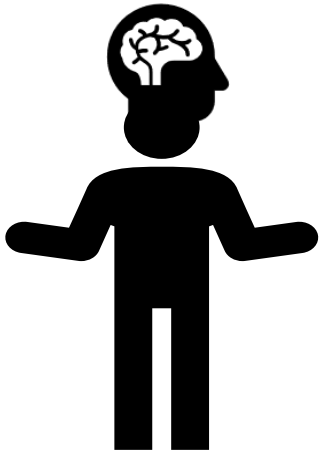
CYBERHIGIENA
przetwarzania danych osobowych w podmiotach leczniczych

dr JAROSŁAW FELIŃSKI
Wykładowca akademicki
Audytor wiodący ISO 27001
Prezes Zarządu SIODO

IODO CONSULTING
Jarosław FELIŃSKI
NIP 6691050971 REGON 321364647

PRYWATNOŚĆ

- **„Prywatność jako osobista chmura”**



Sfera życia prywatnego w opinii prof. Andrzeja Kopffa dzieli się na dwie „podsfery”: **sferę intymnego życia osobistego** oraz **sferę prywatnego życia osobistego**. Poza ich zakresem rozciąga się sfera powszechnej dostępności. Do pierwszej sfery autor zalicza przeżycia osobiste człowieka, o których dana osoba przekazuje informacje je-dynie najbliższym osobom.

ZASADY GENERALNE - ZAWSZE WAŻNE

Prywatność, dobra osobiste a dane osobowe

Konstytucja mówi: art. 47. Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Ustawa Kodeks Cywilny mówi: art. 23. Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

RODO mówi: art. 4 pkt 1) „Dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Ustawa prawo autorskie mówi: Art. 81. 1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego za strzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. 2. Zezwolenia nie wymaga rozpowszechnianie wizerunku: 1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych; 2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza [...].

ZASADY GENERALNE - ZAWSZE WAŻNE

USTAWA z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta

Rozdział 6

Prawo do poszanowania intymności i godności pacjenta

Art. 20. 1. Pacjent ma prawo do poszanowania intymności i godności, w szczególności w czasie udzielania mu świadczeń zdrowotnych.

2. Prawo do poszanowania godności obejmuje także prawo do umierania w spokoju i godności.

Art. 22. 1. W celu realizacji prawa, o którym mowa w art. 20 ust. 1, osoba wykonująca zawód medyczny ma obowiązek postępować w sposób zapewniający poszanowanie intymności i godności pacjenta.

CYBERHIGIENA wg NIS2

motyw

(49) Polityka cyberhigieny stanowi podstawę pozwalającą chronić infrastrukturę sieci i systemów informatycznych, bezpieczeństwo sprzętu, oprogramowania i aplikacji internetowych oraz dane przedsiębiorstw lub użytkowników końcowych wykorzystywane przez podmioty. Polityka cyberhigieny obejmująca wspólny podstawowy zestaw praktyk – w tym aktualizacje oprogramowania i sprzętu, zmianę haseł, zarządzanie nowymi instalacjami, ograniczanie kont dostępu na poziomie administratora oraz tworzenie kopii zapasowych danych – umożliwia utworzenie proaktywnych ram gotowości oraz zapewnienie ogólnego bezpieczeństwa i ochrony w razie incydentów lub cyberzagrożeń. ENISA powinna monitorować i analizować politykę państw członkowskich dotyczącą cyberhigieny.

motyw

(50) Świadomość zagadnień cyberbezpieczeństwa i cyberhigiena mają zasadnicze znaczenie dla podniesienia poziomu cyberbezpieczeństwa w Unii, w szczególności w świetle rosnącej liczby urządzeń podłączonych do internetu, które są coraz częściej wykorzystywane w cyberatakach. Należy dołożyć starań, aby zwiększyć ogólną świadomość ryzyka związanego z takimi urządzeniami, zaś oceny na poziomie Unii mogłyby pomóc w zapewnieniu wspólnego rozumienia takich zagrożeń na rynku wewnętrznym.

PRZEPISY O ZASADACH I WARUNKACH OCHRONY DANYCH OSOBOWYCH

1. Konstytucja Rzeczypospolitej Polskiej z dnia 02 kwietnia 1997 r. (Dz. U. z 1997r., Nr 78 poz. 483 ze zm.) - art. 47 i 51
2. Ustawa z dnia 10 maja 2018r o ochronie danych osobowych (Dz. U 2019, poz. 1781),
3. **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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), Dz. U. UE. L. 2016.119.1 z dnia 4 maja 2016r.,**
4. Ustawa z dnia z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. 2020, poz. 1444)
5. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2020 r. poz. 1740)

PRZEPISY O ZASADACH I WARUNKACH OCHRONY DANYCH OSOBOWYCH

7. Ustawa z dnia 2 grudnia 2009 r. o izbach lekarskich
8. Ustawa z dnia 6 listopada 2008 r. **o prawach pacjenta** i Rzeczniku Praw Pacjenta
9. Ustawa z dnia 28 kwietnia 2011 r. **o systemie informacji** w ochronie zdrowia
10. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty
8. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
9. Ustawa z dnia 6 września 2001 r. – Prawo farmaceutyczne
10. ROZPORZĄDZENIE MINISTRA ZDROWIA z dnia 23 grudnia 2020 r. w sprawie recept
11. USTAWA z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne
12. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, dalej KRI

13. USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz. U. 2018 poz. 1560
14. **DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)**

Podstawy prawne przetwarzania art. 9 RODO

g) przetwarzanie jest niezbędne ze względów związanych z **ważnym interesem publicznym**, na podstawie prawa Unii **lub prawa państwa członkowskiego**, które **są proporcjonalne do wyznaczonego celu,** nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, **diagnozy medycznej,** zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie **z umową z pracownikiem służby zdrowia** i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową; 4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL

Podstawy prawne przetwarzania art. 9 RODO

Art. 9 ust. 2 lit. g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej.

DOSTEPNOŚĆ DO DANYCH
A GWARANCJE ZABEZPIECZENIA TREŚCI DANYCH

W przepisach [wybranych] wprowadzono zapisy o wymaganiach stawianych wykonawcom usług [komercyjnych]  **gromadzących informacje należące do zleceniodawców**

DOSTEPNOŚĆ DO DANYCH

zgodnie z dyspozycją **przepisu art. 28** ust. 2a pkt. 1) uoppirp,
cyt.: „(…) **opłaty** (…), **nie pobiera** się w przypadku udostępnienia dokumentacji medycznej: (…) pacjentowi albo jego przedstawicielowi ustawowemu **po raz pierwszy** w żądanym zakresie i w sposób, o którym mowa w art. 27 ust. 1 pkt 2 i 5 oraz ust. 3 (…)

RODO art. 15 ust 3. Administrator **dostarcza osobie**, której dane dotyczą, **kopię danych osobowych** podlegających przetwarzaniu**.**
Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać i opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię **drogą elektroniczną** i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

PRZYKŁAD w CM UJASTEK

Stan Faktyczny i Decyzja Prezesa UODO

W okresie od 1 do 23 lipca 2023 r. Centrum Medyczne Ujastek w Krakowie wdrożyło monitoring wizyjny na oddziale neonatologii, rejestrując obraz noworodków oraz ich matek podczas intymnych czynności, takich jak karmienie piersią czy pielęgnacja. Co istotne, zarówno pacjenci, jak i personel nie byli świadomi istnienia kamer, co oznacza, że monitoring miał charakter niejawny. Ponadto, dzieci objęte monitoringiem nie wymagały intensywnej terapii, a ich stan zdrowia nie był zagrożony.

W toku postępowania UODO ustalono, że placówka:

- **Nie posiadała podstawy prawnej** do przetwarzania danych osobowych za pomocą monitoringu wizyjnego, co narusza art. 6 i 9 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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 (Dz.Urz. UE L z 2016 r. Nr 119, s. 1; dalej: RODO).
- **Nie spełniła obowiązku informacyjnego** wobec pacjentów i personelu, łamiąc tym samym art. 13 RODO.
- **Nie wdrożyła odpowiednich środków technicznych i organizacyjnych** zabezpieczających nagrania, co jest wymagane na mocy art. 32 RODO.
- **Nie przeprowadziła oceny skutków dla ochrony danych (DPIA)** przed wdrożeniem monitoringu, co stanowi naruszenie art. 35 RODO.

Dodatkowo placówka zgłosiła naruszenie wynikające z zagubienia lub kradzieży kart pamięci z urządzeń rejestrujących obraz, które nie były odpowiednio zabezpieczone (np. przez szyfrowanie). W związku z powyższymi naruszeniami Prezes UODO uznał, że działania podmiotu leczniczego naruszyły przepisy RODO (w szczególności art. 5, 6, 9, 13 oraz 35 RODO) i nałożył na Centrum Medyczne Ujastek łączną karę administracyjną w wysokości 1 145 891,25 zł, podzieloną na:

1. **687 534,75 zł** – za niezgodne z prawem wdrożenie monitoringu.
2. **458 356,50 zł** – za brak odpowiednich środków zabezpieczających, co doprowadziło do incydentu związanego z niezabezpieczonymi kartami pamięci.

PRZYKŁAD

Dla Kontrahenta | Szpital | Projekty i inwestycje | Kariera | Kontakt

Zawiadomienie o naruszeniu ochrony danych osobowych

Szanowni Państwo,

niniejszym w trybie art. 34 Rozporządzenia 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), dr n. med. Michał Zabojszcz, dyrektor SP ZOZ MSWiA w Krakowie informuje, że w dniu 8 marca 2025 r. SP ZOZ MSWiA w Krakowie, będący Administratorem Państwa danych osobowych, zidentyfikował incydent związany z cyberatakiem typu ransomware, który spowodował naruszenie ochrony danych osobowych. Atak polegał na zastosowaniu złośliwego oprogramowania szyfrującego pliki przechowywane na naszych serwerach, co wiąże się z wysokim ryzykiem ich nieuprawnionego dostępu i potencjalnej kradzieży.

W wyniku tego zdarzenia doszło do utraty dostępności danych osobowych, a także, z dużym prawdopodobieństwem, naruszenia ich poufności. Dotyczy to m.in. informacji dotyczących pacjentów, pracowników, kontrahentów oraz innych osób, których dane były przetwarzane przez SP ZOZ MSWiA w Krakowie.

W związku z powyższym podjęto działania zmierzające do likwidacji skutków ataku oraz ustalenia zakresu szkód. Jednocześnie SP ZOZ MSWiA w Krakowie dokonał zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformował uprawnione instytucje, a także złożył zawiadomienie o podejrzeniu popełnienia przestępstwa.

SŁUŻBA ZDROWIA MSWiA

Metadane strony

Autor: Michał Zabojszcz
Dodano: 10 Marca 2025
Zaktualizowano: 23 Marca 2025

PRZYKŁAD

Rodzaje danych objętych atakiem:

1. Dane identyfikacyjne (m.in. imię, nazwisko, PESEL, nr dokumentu stwierdzającego tożsamość, organ wydający oraz data ważności, data urodzenia, obywatelstwo).
2. Dane adresowe (adres zamieszkania, zameldowania, korespondencyjny).
3. Dane kontaktowe (nr telefonu, adres e-mail).
4. Dane szczególnej kategorii o stanie zdrowia (dokumentacja medyczna).
5. W minimalnym zakresie dane dotyczące faktu aresztowania lub zatrzymania przez organy ścigania w zakresie w jakim osobom tym były udzielane świadczenia zdrowotne.
6. Dane finansowe (nr rachunków bankowych, informacja o wysokości wynagrodzenia pracowników i wysokości wynagrodzenia wynikających z umów kontraktowych).
7. Dane kadrowe (historia zatrudnienia, informacje potwierdzające kwalifikacje, dane dzieci i współmałżonków pracowników).

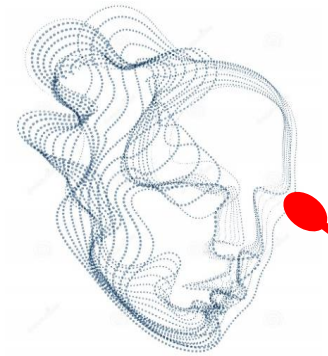
Kategorie osób objętych atakiem:

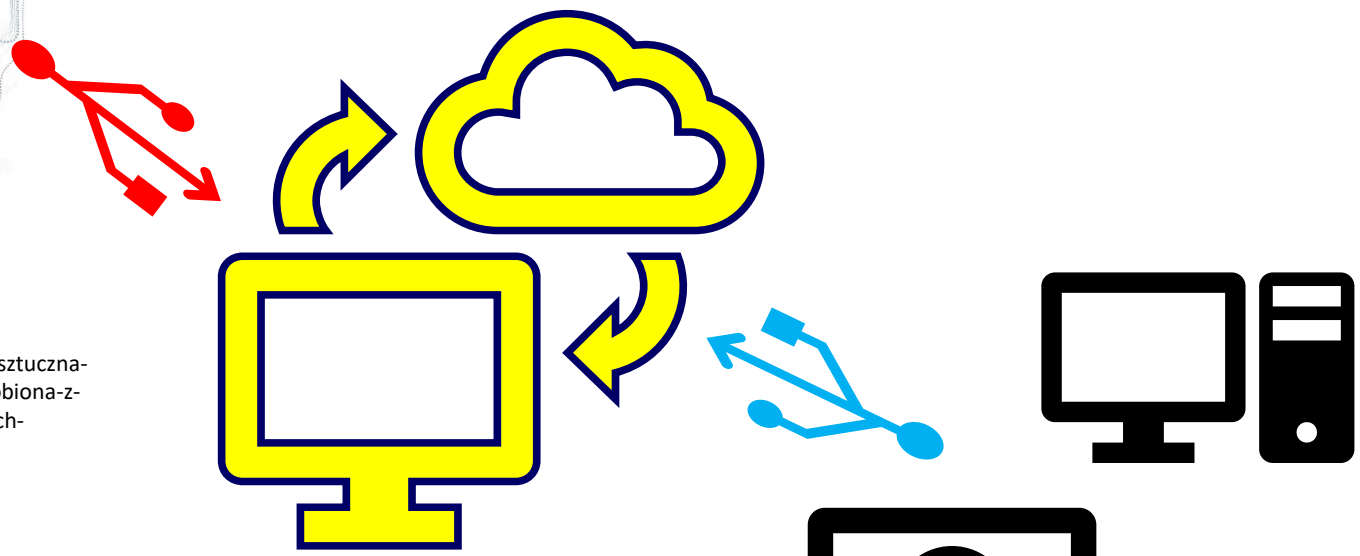
1. Pacjenci i osoby upoważnione przez pacjentów.
2. Pracownicy.
3. Kontrahenci/podwykonawcy.

Obecnie nie możemy jednoznacznie potwierdzić, czy Państwa dane zostały skradzione, jednak istnieje wysokie prawdopodobieństwo. Wciąż trwa analiza skali incydentu, dlatego w trosce o bezpieczeństwo zalecamy dokładne zapoznanie się z poniższymi wskazówkami oraz regularne sprawdzanie aktualnych komunikatów na stronie głównej www.zozmswiakrakow.pl.

„USŁUGI SPOŁECZEŃSTWA INFORMACYJNEGO- CYFRO/HUB”

Open AI ChatGPT





Źródło- https://pl.dreamstime.com/cyfrowa-dusza-maszyny-sztuczna-inteligencja-wizualizacja-g%C5%82owy-cz%C5%82owieka-zrobiona-z-cz%C4%85stek-kropkowanych-przep%C5%82ywaj%C4%85cych-image216958952

e ~ sądy, e ~ administracja;

e ~ WUŚ; e ~ PUAP;

e ~ szkoła; e ~ recepta;

„e ~ L4” itd.; e ~ pacjent;

e ~ student.

e ~ DUKACJA?

DYREKTYWA (UE) 2015/1535 PARLAMENTU EUROPEJSKIEGO I RADY z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie)

„DYLEMAT” ADMINISTRATORA/INSPEKTORA

NARUSZENIE W PODZIALE NA:

naruszenie ochrony danych osobowych – 4/12

naruszenie bezpieczeństwa – 4/12

naruszenia niniejszego rozporządzenia – 28/3/h

naruszenia podstawowych praw lub wolności – 24/1 # 32

naruszenie ochrony danych osobowych – 33/1

naruszenia przepisów o ochronie danych osobowych – (1/ 2. /5)
naruszenia przepisów dotyczących przetwarzania danych osobowych
- 58 UODO

RODO

Artykuł 82 Prawo do odszkodowania i odpowiedzialność

1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2. […]
3. […]
4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

Artykuł 24 / 417 Kodeks Cywilny

Za szkodę odpowiedzialny jest nie tylko ten, kto ją bezpośrednio wyrządził, lecz także ten, kto inną osobę do wyrządzenia szkody nakłonił albo był jej pomocny, jak również ten, kto świadomie skorzystał z wyrządzonej drugiemu szkody.

Art. 24. § 1. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

Art. 417[1]. Jeżeli […] została wyrządzona szkoda na osobie, poszkodowany może żądać całkowitego lub częściowego jej naprawienia oraz zadośćuczynienia pieniężnego za doznaną krzywdę, gdy okoliczności, a zwłaszcza niezdolność poszkodowanego do pracy lub jego ciężkie położenie materialne, wskazują, że wymagają tego względy słuszności.

ZMIANY PRZEPISÓW KRAJOWYCH i UE

USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wraz z naniesionymi zmianami z projektu nowelizacji ustawy z dnia 2 grudnia 2024 roku

ZAŁĄCZNIKI

Załącznik nr 1

SEKTORY KLUCZOWE

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.
		Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu

ZMIANY PRZEPISÓW KRAJOWYCH i UE

Dziennik Urzędowy
Unii Europejskiej

26 MARCA 2025

PL
Seria L

2025/327

5.3.2025

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2025/327

z dnia 11 lutego 2025 r.

w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847

Podstawę EPDZ stanowią ważne istniejące unijne horyzontalne ramy, w tym:

- ogólne rozporządzenie o ochronie danych (RODO)
- akt w sprawie zarządzania danymi
- akt w sprawie danych
- dyrektywa w sprawie bezpieczeństwa sieci i informacji.

EPDZ uzupełnienia te akty i wprowadza przepisy dostosowane do obecnych potrzeb sektora zdrowia. W przypadku **pierwotnego wykorzystania pacjenci będą mieli** prawo do ograniczenia dostępu pracowników służby zdrowia do całości lub części swoich elektronicznych danych osobowych dotyczących zdrowia wymienianych za pośrednictwem infrastruktury EPDZ.

CYBER ZJAWISKA BUDZĄCE NIEPOKÓJ SPOŁECZNY

https://www.google.com/search?sca_esv=cb366a807a68809b&sxsrf=ADLYWIINSQILYpXsebioHhq-PcHRvzvCBQ:1732287640133&q=smartwatch&udm=2&fbs=AEQNm0Dvr3xYvXRaGaB8liPABJYdVC1NjYIFuBO3QJyWQ7GvBqotGuNIL7YJZii2ZN8ynNxI0n-SwmfZ81HoXvsBSMGh14mRmZNZ_ANbUNyCdnz_wYar6wUiN7PwC7F6gCeeoGtwi8SiWvj_9HqTK23c5r8aKxODC0-NkJnOkAhO4aTVIiyzs1nEh3ZTrSjWUFC0zSfxd4mwLYQ89VEOXmrHrVxpK4vUv9Bm24WxEAD2nx_y5SFjeqQ&sa=X&ved=2ahUKEwiymMGrmvCJAxXsHhAIHVbcNYoQtKgLegQIFhAB&biw=1422&bih=621&dpr=1.35

DOROŚLI

CYBER~KROKI

CYBER~KALENDARZ

CYBER~CIŚNIENIE

CYBER~DIETA [PODAWANA Z PUDEŁKA]

CYBER~ŻAROBEK INFLUENCERSKI

CYBER~WIELE INNYCH

CYBER~ODWYK BEZ Wi-Fi

CYBER~"TWORKI"

CYBER~"ESPERAL"

CYBER~DETOKS

Radio Olsztyn

Nastolatki i dorośli. Ekspertki o serialu „Dojrzewanie" w Radiu Olsztyn

MŁODZIEŻ I DZIECI

CYBER~EKSHIBICJONIZM

CYBER~"AJNAUKA"

CYBER~SAMOKSZTAŁCENIE

CYBER~OKALECZENIE

CYBER~"NASIĄKANIE"

CYBER~PATOLOGIE

CYBER~EROTYZACJA

WNIOSKI

- JAKIMI NARZĘDZIAMI NADZOROWAĆ ZASÓB HUB'ÓW
- JAKIE KWALIFIKACJE POWINNI POSIADAĆ ETATOWI Sp.ZBI
- KTO MA KLUCZ DO TEGO MEGA MAGAZYNU – NP. ZDROWIA?
- CZY TREŚĆ INFORMACJI JEST ODPORNA NA ZMODYFIKOWANIE, KTO MA DOSTĘP?
- PRAWNE INSTRUMENTY OGRANICZAJĄCE AI JAKO SKŁADNIKI ODPORNOŚCI INFORMACJI I JAKOŚCI ZARZĄDZANIA BI

ChatGPT proszę … - podaj odpowiedź …

Propozycja kolejnego wydarzenia nieodpłatna

DZIĘKUJĘ
ZA UWAGĘ

dr JAROSŁAW FELIŃSKI

jaroslaw.felinski@gazeta.pl

602-105-852