Zadania podmiotów opieki zdrowotnej

[kluczowych] w świetle

znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa [UoKSC]

dr JAROSŁAW FELIŃSKI

Wykładowca akademicki

Audytor wiodący ISO 27001

Prezes Zarządu SIODO

IODO CONSULTING
Jarosław FELIŃSKI
NIP 6691050971 REGON 321364647

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 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw**
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)**

USTAWA z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innychustaw1) Dz.U. 2026 r. poz. 252

ZMIANY PRZEPISÓW KRAJOWYCH i UE

Załączniki do ustawy z dnia 23 stycznia 2026 r. (Dz. U. poz. 252)

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 (Dz. U. z 2026 r. poz. 156)
		Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia

USTAWA z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innychustaw1) Dz.U. 2026 r. poz. 252

ZMIANY PRZEPISÓW KRAJOWYCH i UE

Art. 49. Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.

SZBI

- 3.03.2026 - opublikowano
- 4.04.2026 - obowiązuje
- 4.10.2026 - zgłoszenie

https://www.linkedin.com/posts/cyberdefence24-pl_atakuj%C4%85cy-za%C5%BC%C4%85dali-od-plac%C3%B3wki-kilku-milion%C3%B3w-activity-7437905272720875520-p0Lj/?utm_medium=ios_app&rcm=ACoAADnS2mgBv79dJosq4sss2drtgCbylgDKbV4&utm_source=social_share_send&utm_campaign=mail

W wyniku weekendowego **cyberataku na Samodzielny Publiczny Wojewódzki Szpital Zespolony** (SPWSZ), doszło do naruszenia danych osobowych pacjentów, osób przez nich upoważnionych, pracowników, a także kontrahentów i podwykonawców współpracujących ze szpitalem.

Według drugiego **komunikatu** placówki w tej sprawie, obecnie prowadzone są **działania mające na celu wyjaśnienie przyczyn zdarzenia oraz ustalenie pełnego zakresu incydentu**. Podejmowane są również działania **ograniczające skutki** ataku.

Naruszenie zostało zgłoszone do **Prezesa Urzędu Ochrony Danych Osobowych**. Złożono też zawiadomienie o podejrzeniu popełnienia przestępstwa.

CyberDefence 24

Szukaj

CYBERBEZPIECZEŃSTWO | ARMIA I SŁUŻBY | POLITYKA I PRAWO | BIZNES I FINANSE

#CyberMagazyn | Wideo | Strefa Pekao SA

Strona główna / Cyberbezpieczeństwo / Cyberataki / Ransomware sparaliżował systemy szpitala w Szczecinie. Wsparcie zapewnia WOT

CYBERATAK - przykład

WIADOMOŚCI

Ransomware sparaliżował systemy szpitala w Szczecinie. Wsparcie zapewnia WOT

Zuzanna Sadowska 12 marca 2026, 16:22 5 min.

Atak ransomware na Szpital Wojewódzki w Szczecinie doprowadził nie tylko do zaszyfrowania części systemów informatycznych, ale również do naruszenia ochrony danych osobowych pacjentów i pracowników placówki. Według komunikatów placówki, cyberprzestępcy mogli uzyskać dostęp do informacji jeszcze przed ich zaszyfrowaniem. !!!!!!!!!

Obecnie trwa analiza incydentu oraz przywracanie działania systemów przy wsparciu specjalistów z Wojsk Obrony Terytorialnej.

CYBERATAK - przykład

https://www.linkedin.com/posts/michal-sajdak_w-szpitalu-wojskowym-niez%C5%82e-yolo-kto%C5%9B-activity-7437054282341867520-TjpA/?utm_medium=ios_app&rcm=ACoAADnS2mgBv79dJosq4sss2drtgCbylgDKbV4&utm_source=social_share_send&utm_campaign=mail

NIELEGALNOŚĆ DOSTĘPU I UDOSTĘPNIENIA

❌ Ktoś zalogował się na swoje konto w szpitalnym programie medycznym (z dostępem do danych medycznych)
❌ Tak zalogowanego kompa udostępnił innej osobie... i poszedł sobie na kawkę

Incydent szpital opisał nieco bardziej formalnie:

105 Kresowy Szpital Wojskowy z Przychodnią Samodzielny Publiczny Zakład Opieki Zdrowotnej w Żarach, informuje, że w dniu 27 lutego 2026 r. w godzinach 16:20–17:00 doszło do naruszenia ochrony Pani/Pana danych osobowych.

Zdarzenie polegało na udostępnieniu przez pracownika służbowego komputera po uprzednim zalogowaniu się do programu medycznego AMMS przy użyciu indywidualnych danych dostępowych (loginu i hasła). Komputer został udostępniony byłej pracownicy, osobie nieuprawnionej. Następnie pracownik opuścił pomieszczenie, pozostawiając wskazaną osobę przy stanowisku komputerowym z aktywną sesją w systemie.

W chwili zdarzenia były pracownik nie był osobą uprawnioną do korzystania z systemu informatycznego AMMS ani do przeglądania dokumentacji medycznej pacjentów Administratora.

W wyniku naruszenia osoba nieuprawniona uzyskała dostęp do systemu informatycznego AMMS, w którym znajdują się Pani/Pana dane osobowe jako pacjenta, w tym: imię i nazwisko, adresu zamieszkania, numeru PESEL, informacje dotyczące stanu zdrowia, w tym rozpoznania oraz zaleceń medycznych.

133 36 komentarzy • 6 udostępnień na LinkedIn

CYBERATAK - przykład

Zawiadomienie o naruszeniu ochrony danych osobowych w Bonifraterskim Centrum Medycznym sp. z o.o. 17 marca 2026

6. Proponowane środki zaradcze – jakie działania możecie Państwo podjąć?

Należy podkreślić, **że obecnie nie ma pewności** czy Państwa dane zostały wykradzione, niemniej jednak zalecamy zachowanie szczególnej czujności i ostrożności, zwracania szczególnej uwagi na nietypowe zdarzenia czy na jakiekolwiek sygnały mogące świadczyć o wykorzystywaniu Państwa danych niezgodnie z przepisami prawa. W związku z ujawnieniem Państwa danych osobowych, możecie Państwo zminimalizować wystąpienie opisanych wyżej ryzyk m.in. poprzez:

1) zastrzeżenie numeru PESEL. Od 1 czerwca 2024 r. instytucje finansowe (np. banki) mają obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki. W dowolnym momencie mogą Państwo cofnąć zastrzeżenie, wykonać przysługujące Państwu czynności a następnie zastrzec numer ponownie. Zastrzeżenie numeru PESEL w żaden sposób nie zablokuje Państwa możliwości rejestracji do lekarza, realizacji recepty czy załatwienia sprawy urzędowej, ale zabezpiecza Państwa przed zawarciem umowy kredytu/pożyczki w Państwa imieniu przez osoby do tego nieuprawnione. **Zastrzec numer PESEL** można na wiele sposobów, w tym elektronicznie, za pośrednictwem Internetu, w aplikacji mObywatel oraz osobiście w urzędzie.,

2) wykupienie rocznego abonamentu tzw. Alertów w BIK (Biurze Informacji Kredytowej). Alerty takie, przychodzą w postaci krótkich wiadomości SMS wysyłanych pod Państwa numery telefonów komórkowych zawsze, gdy ktoś złoży wniosek o kredyt/pożyczkę na Państwa dane lub spróbuje podpisać w Państwa imieniu umowę np. na świadczenie usług telekomunikacyjnych z operatorem sieci komórkowej lub usług RTV z dostawcą sygnału telewizyjnego,

3) przejrzenie dostępnych informacji w Internecie na swój temat i usunięcie tych, które mogą wykorzystać przestępcy do nielegalnej działalności, w szczególności numery telefonów komórkowych, adresy e-mail, wizerunek, adresy zamieszkania, ale także zbędne informacje o miejscach pobytu czy zainteresowaniach i wszelkie inne szczegóły, które mogą zostać wykorzystane przez przestępców do podszywania się pod Państwa,

4) możliwość skorzystania ze środków ochrony dóbr osobistych wskazanych w kodeksie cywilnym i kodeksie postępowania cywilnego. Przysługuje Państwu prawo do wytoczenia **powództwa o ochronę dóbr osobistych na podstawie art. 24 k.c. W pozwie można żądać usunięcia skutków naruszenia. Przysługuje Państwu również prawo roszczenia** o odszkodowanie za powstałą szkodę majątkową lub zadośćuczynienie za poniesioną krzywdę spowodowaną naruszeniem dobra osobistego – prawa do prywatności w zakresie autonomii informacyjnej co do decydowania o ujawnianiu informacji o swojej osobie z art. 23 k.c. w zw. z art. 24 k.c. w zw. z art. 448 k.c. (zadośćuczynienie za naruszenie dobra osobistego),

CYBERATAK - przykład

Zawiadomienie o naruszeniu ochrony danych osobowych w Bonifraterskim Centrum Medycznym sp. z o.o. 17 marca 2026

5) zachowanie **szczególnej rozwagi podczas umieszczania** jakichkolwiek prywatnych danych na swój temat w Internecie. Obecnie zakres przestępczej działalności internetowej jest bardzo szeroki i aktywny,
6) **weryfikację swoich haseł** wykorzystywanych w różnych portalach, sklepach internetowych, kontach pocztowych i ich zmianę w taki sposób by były w każdym takim miejscu niepowtarzalne,
7) weryfikację oraz **odnowienie certyfikatów wykorzystywanych do komunikacji z systemami zewnętrznymi**, w tym certyfikatów używanych przez lekarzy,
8) weryfikację występowania Państwa danych w bazie znanych wycieków danych, za pośrednictwem rządowego portalu https://bezpiecznedane.gov.pl
Jeżeli dowiedzą się Państwo o upublicznieniu, wykorzystaniu lub o jakimkolwiek dalszym ujawnieniu danych osobowych, bardzo proszę o niezwłoczne przekazanie tej informacji do Inspektora Ochrony Danych Bonifraterskiego Centrum Medycznego Sp. z o.o. i/lub o kontakt z najbliższą jednostką Policji lub o zgłoszenie na numer alarmowy 112. Ponadto mają Państwo prawo złożyć zawiadomienie do prokuratury o możliwości popełnienia przestępstwa w związku z wejściem nieuprawnionej osoby w posiadanie Państwa danych osobowych i wykorzystywanie ich w jakikolwiek niedozwolony sposób. Mają Państwo również prawo złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych (00-014 Warszawa, ul. Moniuszki 1a, https://uodo.gov.pl/pl/526/2464).

7. Dane kontaktowe

Inspektor Ochrony Danych:

W razie jakichkolwiek pytań, proszę o kontakt z Inspektorem Ochrony Danych, w osobie Pani Małgorzaty Topyła-Komosa. Z IOD można skontaktować się za pośrednictwem wiadomości e-mail: iodbcm@bonifratrzy.pl.

Administrator danych osobowych:

Bonifraterskie Centrum Medyczne sp. z o.o. z siedzibą we Wrocławiu przy ul. Gen. Traugutta 57/59
KRS: 0000952604, NIP: 8992919206
Biuro Zarządu, Centrum Jasna, ul. Jasna 14/16A, 4 piętro, 00-041 Warszawa

https://bcmbonifratrzy.pl/aktualnosci/zawiadomienie-o-naruszeniu-ochrony-danych-osobowych-w-bonifraterskim-centrum-medycznym-sp-z-o-o/?_gl=1*1l1h966*_up*MQ..*_ga*NjMxMDUwNDQ5LjE3NzM5OTcxODM.*_ga_C1DLTR103E*czE3NzM5OTcxODIkbzEkZzEkdDE3NzM5OTcxOTMkajQ5JGwwJGgw

CYBERATAK - SKUTKI

Artykuł 33
Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W **przypadku naruszenia** ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż **w terminie 72 godzin** po **stwierdzeniu naruszenia** – **zgłasza je organowi nadzorczemu** właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2.Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3.Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
a) **opisywać charakter naruszenia** ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) **opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;**
d) **opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia** naruszeniu ochrony danych osobowych, w tym w **stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków**.
4.Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki
5.Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

1. Porady prawne i konsultacje:

- **Jednorazowa porada prawna:** od 150 zł do 500 zł za 30-60 minut.
- **Analiza dokumentacji:** od 200 zł do 400 zł. Radca Prawn... +2

2. Pisma procesowe i umowy:

- **Proste pisma (wezwania do zapłaty, proste umowy):** od 450 zł do 1500 zł.
- **Pozwy, odpowiedzi na pozew, apelacje:** od 750 zł wzwyż. Marcin Chowani...

3. Prowadzenie sprawy w sądzie (reprezentacja):
Koszty zależą często od wartości

https://spwsz.szczecin.pl/news/zawiadomienie-o-naruszeniu-ochrony-danych-osobowych

SAMODZIELNY PUBLICZNY
WOJEWÓDZKI SZPITAL ZESPOLONY
w Szczecinie

Unia Europejska

szukaj podanej frazy

Strona główna | Aktualności | O nas | Jednostki szpitala | Strefa pacjenta | Projekty | Ogłoszenia (Zamówienia) | RODO | Kontakt

- Strona główna
- Aktualności
- O nas
- Jednostki szpitala
- Strefa pacjenta
- Projekty

11
03.2026

Zawiadomienie o naruszeniu ochrony danych osobowych

Drukuj

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH W SAMODZIELNYM PUBLICZNYM WOJEWÓDZKIM SZPITALU ZESPOLONYM W SZCZECINIE (ARKOŃSKA I ZDUNOWO)

https://spwsz.szczecin.pl/news/zawiadomienie-o-naruszeniu-ochrony-danych-osobowych

6. **PROPONOWANE ŚRODKI ZARADCZE** – JAKIE DZIAŁANIA **MOŻECIE PAŃSTWO** PODJĄĆ?

Należy podkreślić, że obecnie **nie ma pewności czy Państwa dane zostały wykradzione**, niemniej jednak zalecamy zachowanie szczególnej czujności i ostrożności, zwracania szczególnej uwagi na nietypowe zdarzenia czy na jakiekolwiek sygnały mogące świadczyć o wykorzystywaniu Państwa danych niezgodnie z przepisami prawa.

W związku z ujawnieniem Państwa danych osobowych, możecie Państwo zminimalizować wystąpienie opisanych wyżej ryzyk m.in. poprzez:

1) zastrzeżenie numeru PESEL. Od 1 czerwca 2024 r. instytucje finansowe (np. banki) mają obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki. W dowolnym momencie mogą Państwo cofnąć zastrzeżenie, wykonać przysługujące Państwu czynności a następnie zastrzec numer ponownie. Zastrzeżenie numeru PESEL w żaden sposób nie zablokuje Państwa możliwości rejestracji do lekarza, realizacji recepty czy załatwienia sprawy urzędowej, **ale zabezpiecza Państwa przed zawarciem umowy kredytu/pożyczki** w Państwa imieniu przez osoby do tego nieuprawnione. Zastrzec numer PESEL można na wiele sposobów, w tym elektronicznie, za pośrednictwem Internetu oraz osobiście w urzędzie. Wszelkie szczegóły tego jak to zrobić znajdują się na rządowej stronie: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie;

2) wykupienie rocznego abonamentu tzw. Alertów w BIK (Biurze Informacji Kredytowej). Alerty takie, przychodzą w postaci krótkich wiadomości SMS wysyłanych pod Państwa numery telefonów komórkowych zawsze, gdy ktoś złoży wniosek o kredyt/pożyczkę na Państwa dane lub spróbuje podpisać w Państwa imieniu umowę np. na świadczenie usług telekomunikacyjnych z operatorem sieci komórkowej lub usług RTV z dostawcą sygnału telewizyjnego.

3) przejrzenie dostępnych informacji w Internecie na swój temat i usunięcie tych, które mogą wykorzystać przestępcy do nielegalnej działalności, w szczególności numery telefonów komórkowych, adresy e-mail, wizerunek, adresy zamieszkania, ale także zbędne informacje o miejscach pobytu czy zainteresowaniach i wszelkie inne szczegóły, które mogą zostać wykorzystane przez przestępców do podszywania się pod Państwa.

BANK MÓWI NIE !

https://spwsz.szczecin.pl/news/zawiadomienie-o-naruszeniu-ochrony-danych-osobowych

4) możliwość skorzystania ze środków ochrony dóbr osobistych wskazanych w kodeksie cywilnym i kodeksie postępowania cywilnego. Przysługuje Państwu **prawo do wytoczenia powództwa** o ochronę dóbr osobistych na podstawie art. 24 k.c. W pozwie można żądać usunięcia skutków naruszenia. Przysługuje Państwu również **prawo roszczenia o odszkodowanie** za powstałą szkodę majątkową lub zadośćuczynienie za poniesioną krzywdę spowodowaną naruszeniem dobra osobistego – prawa do prywatności w zakresie autonomii informacyjnej co do decydowania o ujawnianiu informacji o swojej osobie z art. 23 k.c. w zw. z art. 24 k.c. w zw. z art. 448 k.c. (zadośćuczynienie za naruszenie dobra osobistego). – **OPŁACA ADWOKATA SZPITAL**

5) zachowanie szczególnej rozwagi podczas umieszczania jakichkolwiek prywatnych danych na swój temat **w Internecie**. Obecnie zakres przestępczej działalności internetowej jest bardzo szeroki i aktywny.

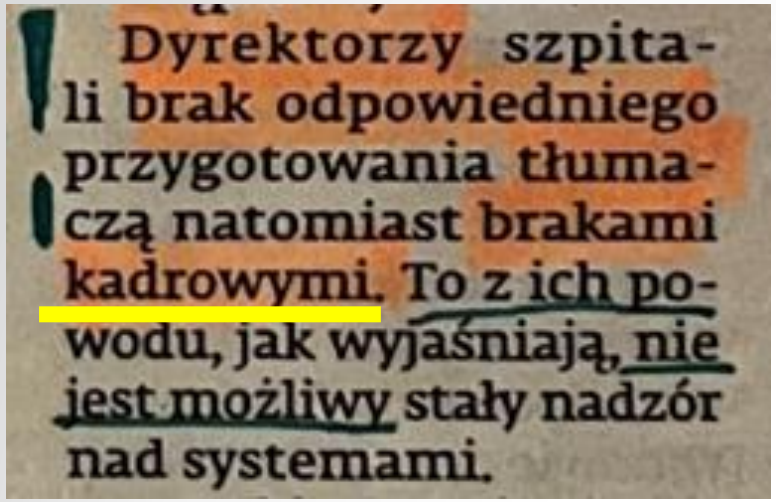
6) weryfikację swoich haseł wykorzystywanych w różnych portalach, sklepach internetowych, kontach pocztowych i ich zmianę w taki sposób by były w każdym takim miejscu niepowtarzalne.

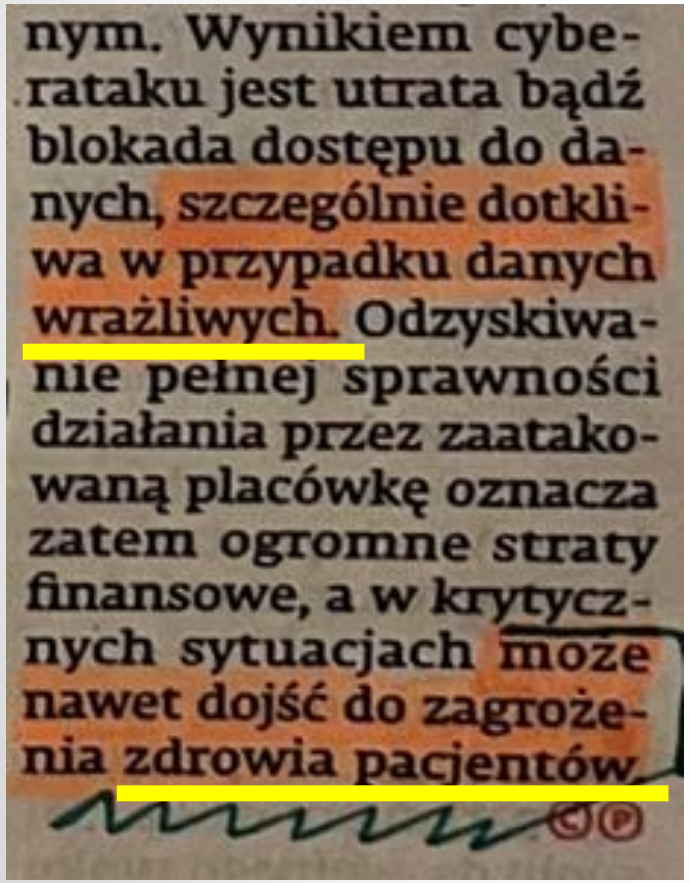
7) weryfikację oraz odnowienie certyfikatów wykorzystywanych do komunikacji z systemami zewnętrznymi, w tym certyfikatów używanych przez lekarzy.

8) weryfikację występowania Państwa danych w bazie znanych wycieków danych, za pośrednictwem rządowego portalu https://bezpiecznedane.gov.pl

Jeżeli dowiedzą się Państwo **o upublicznieniu, wykorzystaniu lub o jakimkolwiek dalszym ujawnieniu** danych osobowych, bardzo proszę o niezwłoczne przekazanie tej informacji do Inspektora Ochrony Danych SPWSZ w Szczecinie i/lub o kontakt z najbliższą jednostką Policji lub o zgłoszenie na numer alarmowy 112.

Ponadto mają Państwo prawo złożyć zawiadomienie do prokuratury o możliwości popełnienia przestępstwa w związku z wejściem nieuprawnionej osoby w posiadanie Państwa danych osobowych i wykorzystywanie ich w jakikolwiek niedozwolony sposób. Mają Państwo również prawo złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Moniuszki 1, https://uodo.gov.pl/pl/526/2464). – **PRZECIWKO SZPITALOWI**


Dyrektorzy szpitali brak odpowiedniego przygotowania tłumaczą natomiast brakami kadrowymi. To z ich powodu, jak wyjaśniają, nie jest możliwy stały nadzór nad systemami.


nym. Wynikiem cyberataku jest utrata bądź blokada dostępu do danych, szczególnie dotkliwa w przypadku danych wrażliwych. Odzyskiwanie pełnej sprawności działania przez zaatakowaną placówkę oznacza zatem ogromne straty finansowe, a w krytycznych sytuacjach może nawet dojść do zagrożenia zdrowia pacjentów.

Szpitale pod cyfrowym ostrzałem. Rekordowa fala ataków hakerskich na placówki medyczne

DGP 12/03/2026

OCHRONA ZDROWIA Krajowe podmioty medyczne **pozostają dla cyberprzestępców łatwym celem.** W 2025 r. liczba incydentów wzrosła o 40 proc., a placówki borykają się z brakami kadrowymi i niedofinansowaniem bezpieczeństwa

Patrycja Otto
patrycja.otto@infor.pl

Weekendowy cyberatak na szpital wojewódzki w Szczecinie, w którym cyberprzestępcy zaszyfrowali dane, tym samym blokując do nich dostęp, po raz kolejny obnażył słabość podmiotów medycznych, dowodząc, jak łatwym są celem. Z roku na rok liczba ataków na szpitale rośnie. W 2025 r., jak wynika z danych zgromadzonych dla DGP przez Sektorowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w Centrum e-Zdrowia (CSIRT CeZ), zarejestrowano rekordową liczbę 1441 incydentów. Oznacza to wzrost aż o 40 proc. względem 2024 r., w którym było ich 1028. Co więcej, po danych z ubiegłego roku widać, że z każdym miesiącem fala coraz bardziej się rozkręca. Do sierpnia 2025 r. było średnio 118 ataków miesięcznie. W ostatnich czterech miesiącach ubiegłego roku ich liczba wzrosła do średnio ponad 123.

Najczęstsze metody

Metody ataków nie zmieniły się w sposób istotny. Wśród najczęstszych typów incydentów w 2025 r. były oszustwa komputerowe (phishing, vishing, socjotechnika), których zarejestrowano w sumie 580 wobec 374 w 2024 r., oraz wykryte podatności, które mogą zostać wykorzystane w ataku – 344 incydenty wobec 242 w 2024 r.

– Widać więc, że atakujący nie zmieniają sposobów działania, natomiast doskonalą swoje metody i intensyfikują te, które wykorzystywali dotychczas – informuje Tomasz Kulas, dyrektor departamentu komunikacji i promocji, rzecznik Centrum e-Zdrowia.

Jak mówi Kamil Sadkowski, ekspert cyberbezpieczeństwa ESET, ataki ransomware, jak ten w Szczecinie, są jedną z najpopularniejszych i coraz częściej wykorzystywanych metod cyberprzestępców. Do tego Polska jest wśród najczęściej atakowanych w ten sposób państw na świecie – obok Turcji i Stanów Zjednoczonych.

Nasilenie ataków wynika z kilku przyczyn.

Po pierwsze, z rozwoju modelu Ransomware as a Service. Wyspecjalizowane grupy tworzą złośliwe oprogramowanie i udostępniają je atakującym. Jak tłumaczy Kamil Sadkowski, obniża to próg wejścia i sprawia, że nawet mało zaawansowani technicznie przestępcy mogą przeprowadzać skuteczne ataki.

Po drugie, w obecnej sytuacji geopolitycznej Polska jest celem wzmożonej aktywności profesjonalnych, wysoko zorganizowanych grup powiązanych z rządami (tzw. grup APT). Ataki na infrastrukturę krytyczną są natomiast jednym z podstawowych sposobów ich działania.

Po trzecie, jak zauważają eksperci, nie bez znaczenia jest niewystarczający poziom zabezpieczenia placówek medycznych. I nie chodzi tylko o pieniądze, choć dostęp do nich wciąż jest za mały. Mimo oferowania coraz to nowych programów wsparcia, np. w postaci konkursów w ramach programu Cyfrowa Europa, dostęp do nich wciąż jest za mały. Inicjatywa ma na celu sfinansowanie najpilniejszych potrzeb w zakresie bezpieczeństwa IT – od testów penetracyjnych w szpitalach przez zaawansowaną sztuczną inteligencję aż po ochronę podmorskich kabli. Daje dostęp do dotacji na cyberbezpieczeństwo, sięgające w niektórych przypadkach nawet 75 proc. kosztów projektu. Termin składania wniosków upływa 31 marca 2026 r.

Luki w bezpieczeństwie

Permanentnym problemem, jak mówi Piotr Zielaskiewicz, menedżer DAGMA Bezpieczeństwo IT, pozostaje jednak niedobór bieżących środków na cyberbezpieczeństwo. To sprawia, że choć pewien poziom zabezpieczeń bywa osiągany, to jego utrzymanie i rozwój pozostają wyzwaniem. Do tego niezmiennie, jak dodaje, człowiek pozostaje jednym ze słabszych ogniw cyfrowego bezpieczeństwa. Wskazują na to również badania przeprowadzone w szpitalach przez CSIRT CeZ. Wynika z nich, że 60 proc. podmiotów w ogóle nie monitoruje pojawiających się podatności, niecałe 60 proc. wykonuje cykliczne testy kopii i odzyskiwania, a prawie 9 proc. nie ma tak podstawowych mechanizmów ochrony jak oprogramowanie antywirusowe, systemy typu EDR/XDR (analiza zagrożeń na urządzeniach końcowych oraz w sieci) czy firewall. Jak zauważają eksperci, mimo nasilających się cyberataków wciąż też nie jest powszechne logowanie wieloetapowe, czyli proces bezpieczeństwa, w którym użytkownik musi podać co najmniej dwa różne rodzaje poświadczeń, aby uzyskać dostęp do systemu.

Dyrektorzy szpitali brak odpowiedniego przygotowania tłumaczą natomiast brakami kadrowymi. To z ich powodu, jak wyjaśniają, nie jest możliwy stały nadzór nad systemami.

– Ataki zdarzają się nie tylko w godzinach pracy administracji, lecz przez całą dobę. Do pełnego zabezpieczenia placówki konieczne jest zatem posiadanie ekspertów, którzy będą pozostawać w gotowość do działania przez cały czas. W sytuacji, kiedy placówki medyczne borykają się z kłopotami finansowymi, ich pozyskanie jest ogromnym wyzwaniem. Szczególnie, że o najlepszych trzeba konkurować wynagrodzeniem z innymi przedsiębiorstwami i firmami prywatnymi, które są w stanie zapłacić więcej niż walczące permanentnie z płynnością szpitale – mówi dyrektor jednego ze szpitali, dodając, że cały czas stara się zatrudnić dodatkowe osoby, ale bezskutecznie.

Jakie to oznacza straty dla systemu? Te nie zostały policzone. Jak tłumaczy CeZ, są to informacje, których w ramach obsługi incydentów zwykle centrum nie uzyskuje. Średni koszt naruszenia danych w sektorze ochrony zdrowia na świecie był szacowany w 2025 r. na 7,42 mln dol. To najwyższy wskaźnik strat finansowych, przewyższający podobne incydenty w sektorze finansowym, przemysłowym czy energetycznym. Wynikiem cyberataku jest utrata bądź blokada dostępu do danych, szczególnie dotkliwa w przypadku danych wrażliwych. Odzyskiwanie pełnej sprawności działania przez zaatakowaną placówkę oznacza zatem ogromne straty finansowe, a w krytycznych sytuacjach może nawet dojść do zagrożenia zdrowia pacjentów.

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.

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.

PRZESŁANKA A PODSTAWA PRAWNA

PRZESŁANKA RODO

Przesłanka prawna to określony w przepisach warunek faktyczny lub prawny, od którego zaistnienia (lub braku) ustawa uzależnia powstanie, zmianę lub ustanie stosunku prawnego,

PRZYKŁAD

Artykuł 6 Zgodność przetwarzania z prawem
1.Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: […]
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; [SZPITAL]

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

PODSTAWA PRAWNA

PACJENT

Podstawa prawna to konkretny przepis lub zbiór przepisów (ustaw, rozporządzeń), na których opiera się legalność działań.
PRZYKŁAD
Art. 25. 1. Dokumentacja medyczna zawiera co najmniej:
1) oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości:
a) nazwisko i imię (imiona),
b) datę urodzenia,
c) oznaczenie płci,
d) adres miejsca zamieszkania
e) numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość,
f) w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania;

PRACOWNIK

Kadry
- np. - art. 22¹ §1 ustawy Kodeks Pracy kandydatów do pracy
- art. 22¹ § 2-3 ustawy Kodeks Pracy pracowników
- art. 2 ust. 1 pkt 3) ustawy z dnia 4 października 2018 r. o pracowniczych planach kapitałowych – PPK [ZUS, US]
- art. 12 ustawy z dnia 27 czerwca 1997 r. o służbie medycyny pracy i rozporządzenie w tej sprawie oraz inne powiązane
- art. 21 ust. 1 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym

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

CYBER

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.

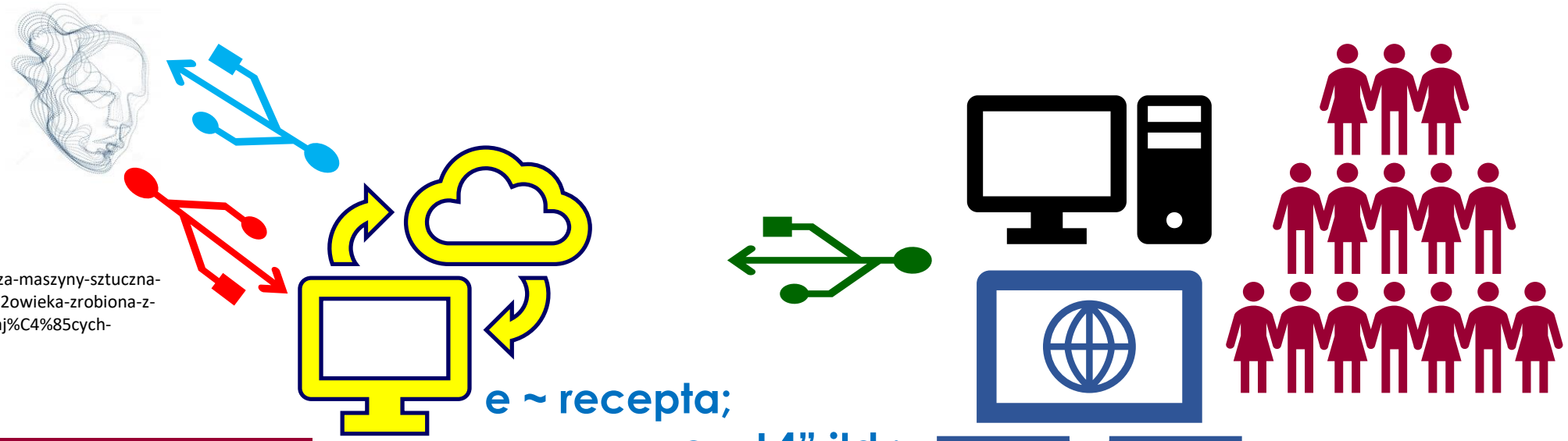
DOSTEPNOŚĆ DO DANYCH

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.

„USŁUGI SPOŁECZEŃSTWA INFORMACYJNEGO- CYFRO/HUB”

LEKARSKI
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 ~ recepta;
„e ~ L4” itd.;
e ~ pacjent;

e ~ DUKACJA?

Art. 8e. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, raz w roku kalendarzowym przechodzi szkolenie.

2. Zakres szkolenia obejmuje wykonywanie obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15.

3. Udział w szkoleniu jest udokumentowany.

Ustawa z dnia 23 stycznia 2026 r. ustaw1) o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych

Art. 8d. Kierownik podmiotu kluczowego lub podmiotu ważnego:

1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie;

2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa; - jak w RODO

3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie;

4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie;

5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.

Art. 8e. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, raz w roku kalendarzowym przechodzi szkolenie.

2. Zakres szkolenia obejmuje wykonywanie obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15.

3. Udział w szkoleniu jest udokumentowany.

Art. 73a – Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 300 % otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

CYFROWY ~ MONITORING WIZYJNY

Art. 23a. 1. Kierownik podmiotu wykonującego działalność leczniczą może określić w regulaminie organizacyjnym sposób obserwacji pomieszczeń:

1) ogólnodostępnych, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pacjentów lub pracowników,

2) w których są udzielane świadczenia zdrowotne oraz pobytu pacjentów, w szczególności pokoi łóżkowych, pomieszczeń higieniczno-sanitarnych, przebieralni, szatni, jeżeli wynika to z przepisów odrębnych,

3) w których są udzielane świadczenia zdrowotne, jeżeli jest to konieczne w procesie leczenia pacjentów lub do zapewnienia im bezpieczeństwa – w przypadku szpitali, zakładów opiekuńczo-leczniczych, zakładów pielęgnacyjno-opiekuńczych, zakładów rehabilitacji leczniczej i hospicjów

– za pomocą urządzeń umożliwiających rejestrację obrazu (monitoring), uwzględniając konieczność poszanowania intymności i godności pacjenta, w tym przekazywanie obrazu z monitoringu w sposób uniemożliwiający ukazywanie intymnych czynności fizjologicznych, potrzebę zastosowania monitoringu w danym pomieszczeniu oraz konieczność ochrony danych osobowych.

1a. Kierownik podmiotu wykonującego działalność leczniczą odpowiada za wykorzystywanie monitoringu zgodnie z przepisami prawa.

Urządzenia własne

Urządzenia zewnętrzne
Umowy zgodnie z RODO

Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej

ZADANIE ADMINISTRATORA/INSPEKTORA

NARUSZENIE W PODZIALE NA:

naruszenie ochrony danych osobowych – 4/12

naruszenie bezpieczeństwa – 4/12

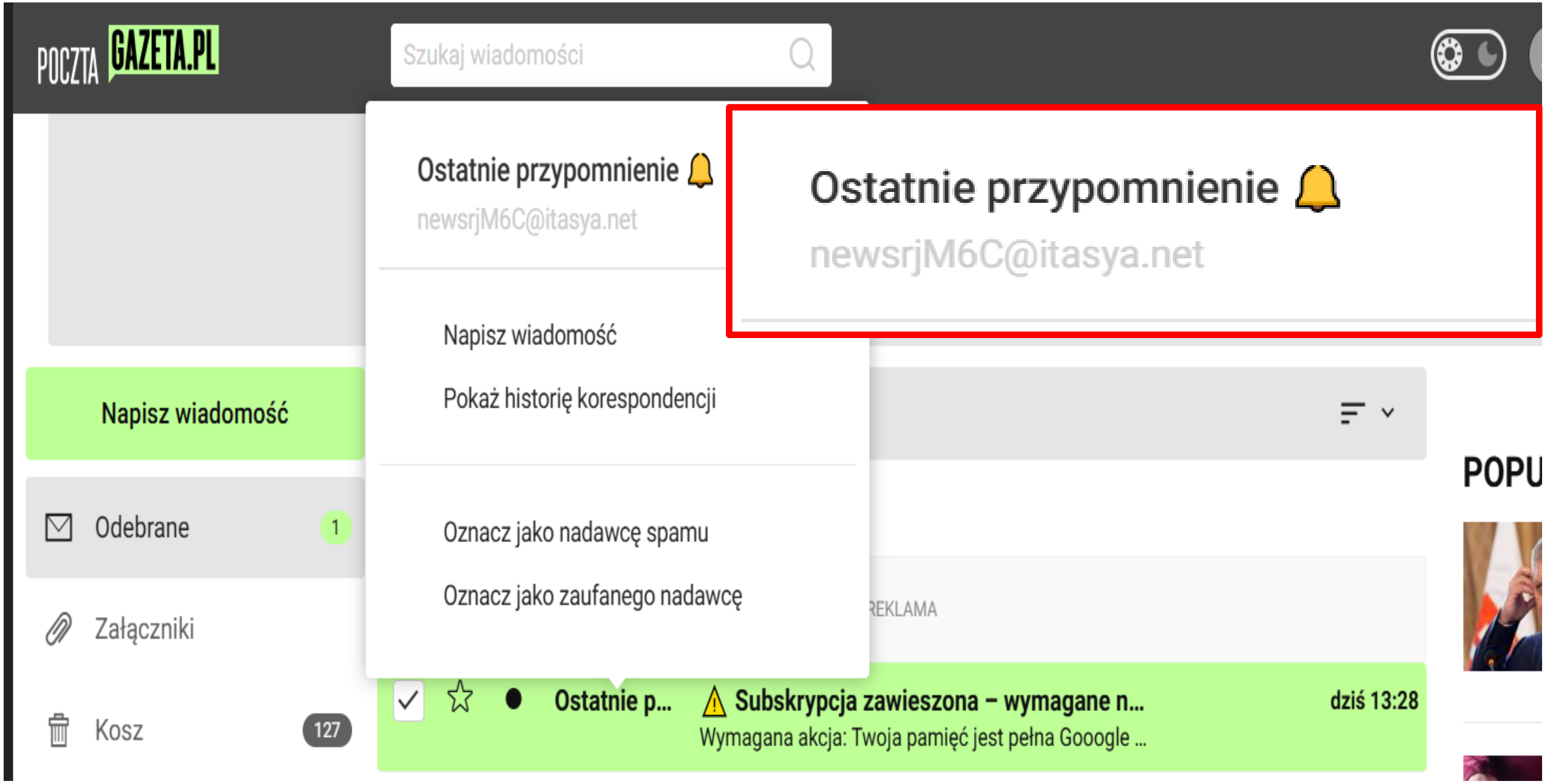
naruszenia niniejszego rozporządzenia – 28/3/h

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

Fałszywe informacje - cyberzagrożenia



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

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.

DZIĘKUJĘ
ZA UWAGĘ

dr JAROSŁAW FELIŃSKI
jaroslaw.felinski@gazeta.pl
602-105-852

dr JAROSŁAW FELIŃSKI – doktor nauk o zarządzaniu i jakości (bezpieczeństwem informacji), MBA w administracji publicznej, aktywny audytor wiodący ISO 27001 [TUV NORD], praktyk, ochroną danych osobowych zajmuje się od 2004 roku, wykładowca wyższych uczelni. Konsultant i wykładowca na studiach podyplomowych z problematyki jakościowego zarządzania bezpieczeństwem informacji: Uniwersytetu Jagiellońskiego w Krakowie; AGH Kraków; Dolnośląskiej Szkoły Wyższej Wrocław; WIT Warszawa. Twórca autorskiego programu podyplomowych studiów zarządzania bezpieczeństwem informacji dla ABI 2013 i IODO 2017– kierownik studiów podyplomowych w roku akademickim od 2013 – 2017/2018. Autor programu studiów podyplomowych **„Menedżer Bezpieczeństwa Informacji”** https://mbi.agh.edu.pl/. Audytor Wiodący PN ISO/IEC 27001. Prezes Stowarzyszenia Inspektorów Ochrony Danych Osobowych. Redaktor naczelny pisma Menedżer Bezpieczeństwa Informacji.