

Obowiązki w zakresie cyberbezpieczeństwa Systemów Elektronicznej Dokumentacji Medycznej, które nie są wyrobem medycznym

dr Jarosław Greser

SYSTEM EDM

oprogramowanie,
lub połączenie
urządzenia
i oprogramowania



przechowywanie,
pośredniczenie
w udostępnianiu,
eksport, import,
konwersję, edycję
lub przeglądanie
elektronicznych



elektronicznych
danych osobowych
dotyczących
zdrowia należących
do priorytetowych
kategorii



przewidziane przez
producenta do
używania przez
świadczeniodawców
podczas
świadczenia opieki
nad pacjentami lub
przez pacjenta
w celu uzyskania
dostępu do jego
danych dotyczących
zdrowia

SYSTEM EDM

Może mieć elementy fizyczne, takie jak urządzenia Internetu Rzeczy lub serwery, ale nie może składać się wyłącznie z takich elementów;

Pozwala na przetwarzanie danych osobowych dotyczących zdrowia i dane genetycznych przetwarzanych w formie elektronicznej (art. 2 ust. 1 lit. a EHDS), ale ich źródło może być szersze niż wyłącznie elektroniczna dokumentacja medyczna zdefiniowana w art. 2 ust. 1 lit. j EHDS;

Może być przeznaczony od używania zarówno przez profesjonalistów, jak i pacjentów;

System EDM nie musi być systemem AI wysokiego ryzyka zgodnie z rozporządzeniem 2024/1689;

System EDM nie obejmuje ogólnego oprogramowania wykorzystywanego w obszarze opieki zdrowotnej. Zgodnie z Motywem 38 są to m.in. programy do przetwarzania tekstu czy zarządzania bazami danych.

ZHARMONIZOWANE KOMPONENTY OPROGRAMOWANIA SYSTEMÓW EDM

Europejski komponent interoperacyjności systemów EDM



komponent oprogramowania systemu EDM

dostarcza i pobiera elektroniczne dane osobowe dotyczące zdrowia

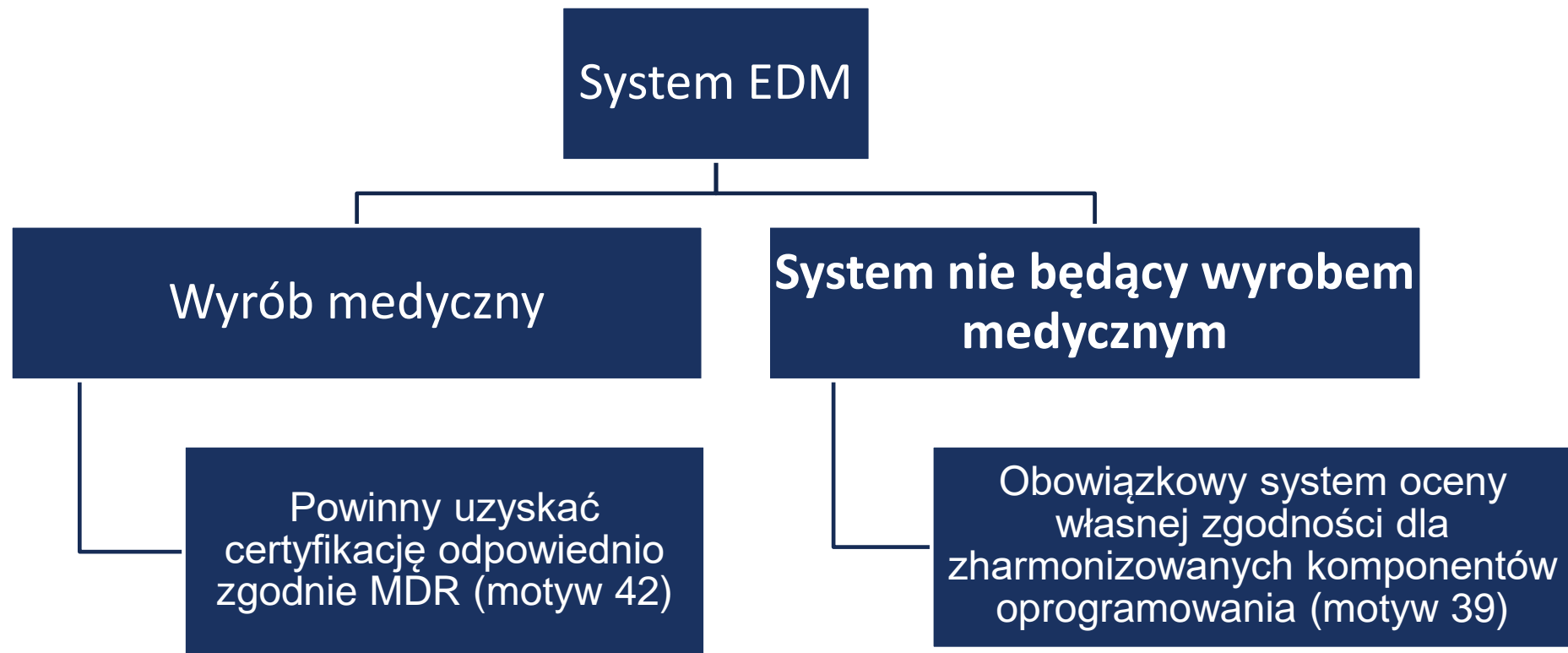
Europejski komponent logowania systemów EDM



komponent oprogramowania systemu EDM

dostarcza informacji o logowaniu w odniesieniu do dostępu pracowników służby zdrowia lub innych osób fizycznych

SYSTEM EDM



CYBERBEZPIECZEŃSTWO SYSTEMÓW EDM

Zgodność z zasadniczymi wymaganiami

art. 30 ust. 1 lit. a +
załącznik II

Projektowanie w sposób, aby ich stosowanie nie stanowiło zagrożenia dla bezpieczeństwa pacjenta o interoperacyjność (punkt 1.1) i kompatybilność były niezawodne i bezpieczne (punkt 1.4).

Zgodność ze wspólnymi specyfikacjami

art. 36.

Akt wykonawczy Komisji, który ma być przyjęty do 26 marca 2027 r.

Inne przepisy

Motyw 36

„bardziej ogólne zabezpieczenia powinny być obsługiwane przez inne mechanizmy”

ZGODNOŚĆ Z ZASADNICZYMI WYMAGANIAMI

Przyjęcie odpowiedzialności przez producenta

art. 39 ust. 5

Samocena w ramach deklaracji zgodności CE

Uprawnienia organu nadzoru rynku

art. 44 ust. 1

Możliwość przeprowadzenia oceny w przypadku podejrzenia ryzyka ryzyko dla (...) ochrony danych osobowych

Uprawnienia organu nadzoru rynku

Zgłaszanie incydentów z zachowaniem wymogów z NIS 2 (art. 44 ust. 7)

Tymczasowy zakaz lub ograniczenie udostępniania sytemu lub wycofanie z obrotu (art. 45 ust. 2)

ZGODNOŚĆ Z ZASADNICZYMI WYMAGANIAMI

Motyw 36: „Zasadnicze wymagania dotyczące bezpieczeństwa tych zharmonizowanych komponentów oprogramowania systemów EDM powinny obejmować elementy specyficzne dla systemów EDM, gdyż bardziej ogólne zabezpieczenia **powinny być obsługiwane przez inne mechanizmy**”

INNE PRZEPISY

Przepisy horyzontalne

Dyrektywa NIS 2

- Ustawa o krajowym systemie cyberbezpieczeństwa
- Sektor kluczowy: ochrona zdrowia m.in.
 - Podmiot leczniczy
 - Laboratoria referencyjne UE
 - Świadczeniodawcy posiadający w swojej strukturze organizacyjnej SOR
- Identyfikacja art. 5: przewyższanie wymogów dla średnich przedsiębiorstw chyba, że **podmiot krytyczny**

Akt o cyberbezpieczeństwie

- Zapowiadał powstanie systemu certyfikacyjnego w dziedzinie cyberbezpieczeństwa, który jest niezależny od innych funkcjonujących systemów
- Brak znaczących postępów
- Propozycja nowelizacji 20 stycznia 2026 r.

INNE PRZEPISY

Wybrane przepisy sektorowe

<p>Akt w sprawie sztucznej inteligencji</p> <ul style="list-style-type: none">• Wyłącznie do systemów AI wysokiego ryzyka• Zasadnicza część obowiązków spoczywa na dostawcy	<p>Akt o cyberodporności</p> <ul style="list-style-type: none">• Spełnienie zasadniczych wymogów• Zasada odstępstwa art. 11	<p>RODO</p> <ul style="list-style-type: none">• Art. 5, 24, 32• Współpraca organu nadzoru rynku z organem nadzorczym w przypadku naruszeń z zakresu ochrony danych osobowych art. 44 ust. 6	<p>Dyrektywa CER</p> <ul style="list-style-type: none">• Rozporządzenie Delegowane Komisji 2023/2450• Świadczeniodawcy, o ile zostaną zaliczeni do grupy podmiotów krytycznych.• Zgodnie z art. 6 ust. 1 ma mieć to miejsce do dnia 17 lipca 2026 r.
--	--	--	--

Dziękuję za uwagę!

dr Jarosław Greser

E-mail: jaroslaw.greser@uwr.edu.pl

The Centre for IT & IP Law, **KU Leuven**

Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, **Uniwersytet Wrocławski**

