



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

DIL/ 2734 /2026

Wrocław, dnia 14 października 2026 roku

Naczelna Rada Lekarska
ul. Jana Sobieskiego 110
00-764 Warszawa

W imieniu Dolnośląskiej Rady Lekarskiej we Wrocławiu, z inicjatywy Komisji Legislacyjnej DRL zwracam się z wnioskiem o podjęcie przez Naczelną Radę Lekarską działań legislacyjnych w sprawie bezpieczeństwa systemów teleinformatycznych służących prowadzeniu dokumentacji medycznej i ochrony podmiotów wykonujących działalność leczniczą jako administratorów danych

I. Przedmiot wniosku

Dolnośląska Izba Lekarska wnosi o podjęcie przez Naczelną Radę Lekarską stanowiska oraz działań określonych w części VIII niniejszego wniosku, w związku z naruszeniami ochrony danych osobowych ujawnionymi w 2026 r. u dostawców oprogramowania służącego prowadzeniu dokumentacji medycznej. Przedmiotem wniosku jest zagadnienie systemowe: prawo nakłada na podmioty wykonujące działalność leczniczą obowiązek prowadzenia dokumentacji medycznej w postaci elektronicznej oraz zapewnienia wymiany danych za pośrednictwem systemów publicznych, czyniąc dla w/w małych podmiotów standaryzowany system komercyjny jedyną realnie dostępną drogą wykonania tych obowiązków. Jednocześnie ocena bezpieczeństwa takiego systemu pozostaje w całości obowiązkiem podmiotu leczniczego, przy braku sektorowego mechanizmu niezależnej weryfikacji, na którym ocena ta mogłaby się oprzeć. Obowiązujące przepisy przenoszą na podmiot wykonujący działalność leczniczą dwa odrębne zadania: **zdefiniowanie** wymaganego poziomu bezpieczeństwa — wobec otwartego pojęcia „wystarczających gwarancji” z art. 28 ust. 1 rozporządzenia 2016/679 — oraz **sprawdzenie**, czy dostawca ten poziom osiąga. Oba zadania powierzono stronie o najmniejszych możliwościach ich wykonania. W ocenie Izby oba powinny zostać przeniesione. Określenie minimalnych wymogów bezpieczeństwa dla systemów przetwarzających dane szczególnej kategorii należy do państwa, które dysponuje właściwymi kompetencjami, a nie do indywidualnej praktyki lekarskiej. Weryfikacja ich dochowania należy do akredytowanej jednostki oceniającej zgodność, a nie do lekarza ani do deklaracji własnej producenta. Podmiotowi wykonującemu działalność leczniczą pozostaje wówczas obowiązek proporcjonalny do jego możliwości: wybór dostawcy spośród zweryfikowanych i udokumentowanie tego wyboru. Izba wnosi zatem, aby na rynku systemów służących prowadzeniu dokumentacji medycznej

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

mogli występować wyłącznie dostawcy spełniający ustawowo określone i niezależnie zweryfikowane wymogi bezpieczeństwa. Ramy prawne pozwalające to osiągnąć w znacznej części już istnieją: ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa pozwala ustanowić schemat certyfikacji rozporządzeniem, a art. 56 ust. 2 rozporządzenia (UE) 2019/881 dopuszcza, by prawo krajowe uczyniło certyfikację obowiązkową.

II. Stan faktyczny

W 2026 r. ujawniono dwa naruszenia ochrony danych u niezależnych dostawców oprogramowania medycznego.

1. Naruszenie u dostawcy MyDr, do którego doszło w okresie 24 czerwca – 1 lipca 2026 r. Platforma obsługuje około 12 tys. placówek medycznych. Prezes Urzędu Ochrony Danych Osobowych wszczął kontrole sektorowe.

2. Naruszenie w systemie Medyc (producent: Qbusoft sp. z o.o.). Do pozyskania danych doszło w dniach 22–23 sierpnia 2026 r., incydent wykryto 8–9 września 2026 r., a upubliczniono 24 września 2026 r. Qbusoft przekazał materiały dotyczące incydentu Policji 9 września i Prezesowi UODO 10 września 2026 r. Prezes UODO zapowiedział kontrolę dostawcy. Dostawca potwierdził pozyskanie imion, nazwisk, numerów PESEL, adresów, numerów telefonów i adresów poczty elektronicznej, uznając za prawdopodobne pozyskanie również kart informacyjnych leczenia szpitalnego. Co do liczby osób dotkniętych naruszeniem źródła nie są zgodne: sprawcy twierdzą, że pozyskali dane 5 mln pacjentów, natomiast według szacunku serwisu Zaufana Trzecia Strona naruszenie mogło dotyczyć około 1 mln osób. Żadna z tych liczb nie została potwierdzona przez dostawcę, organy państwa ani CSIRT Centrum e-Zdrowia. Argumentacja niniejszego wniosku nie opiera się na skali naruszeń ani na ich technicznej przyczynie. Według stanu na dzień sporządzenia wniosku nie opublikowano zweryfikowanych ustaleń pozwalających przypisać któremukolwiek z tych naruszeń konkretny wektor ataku. Podstawą wniosku jest okoliczność, że w ciągu jednego kwartału doszło do dwóch naruszeń, u dwóch niezależnych dostawców tego samego segmentu rynku — segmentu, od którego podmioty lecznicze są uzależnione z mocy prawa. Konsekwencje dotyczą już konkretnych placówek. Jak podano publicznie (money.pl, wrzesień 2026 r.), pacjent poszkodowany naruszeniem w systemie MyDr skierował powództwa przeciwko trzem placówkom medycznym, żądając po 10 tys. zł od każdej. Powództwa nie skierowano przeciwko dostawcy systemu. Wytoczenie powództwa nie rozstrzyga o odpowiedzialności pozwanych; wskazuje natomiast, przeciwko komu roszczenia tego rodzaju są kierowane, co wynika z konstrukcji odpowiedzialności omówionej w części VI.

III. Obowiązki podmiotu wykonującego działalność leczniczą dotyczące dokumentacji medycznej

1. Postać elektroniczna dokumentacji

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570
NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233
Legnica – pl. Słowiański 1, 59-220 Legnica
Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

Zgodnie z § 1 ust. 1 rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2024 r. poz. 798, z 2025 r. poz. 931 i 1853 oraz z 2026 r. poz. 758 i 876), wydanego na podstawie art. 30 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, dokumentacja medyczna jest prowadzona w postaci elektronicznej. Stosownie do § 1 ust. 2 tego rozporządzenia dokumentacja może być prowadzona w postaci papierowej, jeżeli przepis rozporządzenia tak stanowi lub warunki organizacyjno-techniczne uniemożliwiają prowadzenie jej w postaci elektronicznej.

2. Elektroniczna dokumentacja medyczna i jej wymiana

Elektroniczna dokumentacja medyczna została zdefiniowana w art. 2 pkt 6 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2026 r. poz. 208), a jej rodzaje określają przepisy wydane na podstawie art. 13a tej ustawy. Art. 11 ust. 1 ustawy zobowiązuje usługodawców do prowadzenia elektronicznej dokumentacji medycznej, a art. 11 ust. 1b — do dokonywania jej wymiany zgodnie ze standardami zamieszczonymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia. Art. 56 ust. 4 ustawy zobowiązuje usługodawców do zapewnienia możliwości dokonywania wymiany danych zawartych w elektronicznej dokumentacji medycznej za pośrednictwem Systemu Informacji Medycznej, od 1 lipca 2021 r. Odrębny obowiązek przekazywania do tego systemu danych zdarzenia medycznego, również od 1 lipca 2021 r., wynika z art. 56 ust. 2a.

3. Faktyczna droga wykonania obowiązku

Przepisy określają wymagany rezultat — postać elektroniczną, obowiązujące formaty, interoperacyjność oraz zdolność wymiany danych — nie przesądzając modelu organizacyjnego, w którym rezultat ten ma zostać osiągnięty. Dla znacznej części małych podmiotów leczniczych skorzystanie ze standaryzowanego systemu komercyjnego, utrzymywanego przez zewnętrznego dostawcę w roli podmiotu przetwarzającego, stanowi jednak jedyną realnie dostępną organizacyjnie i ekonomicznie drogę wykonania tych obowiązków. Praktyka lekarska prowadzona przez jednego lub kilku lekarzy nie utrzymuje własnej infrastruktury serwerowej, nie dysponuje zespołem utrzymania systemów teleinformatycznych ani nie realizuje samodzielnie integracji z Systemem Informacji Medycznej. Obowiązek jest bezwzględny co do rezultatu, a w realiach tej skali działalności wybór drogi jego wykonania jest w ocenie Izby iluzoryczny.

IV. Brak sektorowego mechanizmu weryfikacji bezpieczeństwa dostawcy

1. Dopuszczenie do rynku

Rozpoczęcie działalności polegającej na dostarczaniu oprogramowania do prowadzenia dokumentacji medycznej nie wymaga licencji, zezwolenia, wpisu do rejestru branżowego ani wykazania kompetencji w zakresie bezpieczeństwa informacji. Obowiązek oceny zgodności jako wyrobu medycznego zależy od

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

przeznaczenia nadanego przez producenta oraz od funkcji konkretnych modułów oprogramowania (art. 2 pkt 1 oraz załącznik VIII, w szczególności reguła 11 rozporządzenia (UE) 2017/745; wytyczne MDCG 2019-11). Oprogramowanie służące prowadzeniu dokumentacji, planowaniu wizyt i rozliczaniu świadczeń zwykle tej kwalifikacji nie spełnia, choć poszczególne moduły analizujące dane lub wspierające decyzje kliniczne mogą jej podlegać.

2. Nadzór w toku działalności

Zadania Centrum e-Zdrowia obejmują budowę, wdrażanie, rozwój i utrzymanie systemów teleinformatycznych będących własnością państwa, w tym Systemu Informacji Medycznej. Wymogi stawiane dostawcom w związku z integracją z tym systemem dotyczą zgodności formatu wymiany danych (HL7 CDA w polskiej implementacji narodowej) oraz zabezpieczenia kanału komunikacji. Wymogi te nie obejmują kompleksowej oceny cyberbezpieczeństwa infrastruktury i organizacji dostawcy ani nie stanowią sektorowego dopuszczenia go do rynku. Centrum e-Zdrowia wskazało to publicznie: *„Zabezpieczenie systemu informatycznego leży po stronie dostawcy – firmy świadczącej daną usługę”* (cyt. za: K. Nocuń, *Dane medyczne a prywatna firma: co z nadzorem, certyfikacją? Centrum e-Zdrowia odpowiada*, Rynek Zdrowia, 14 sierpnia 2026 r.). Nadzór nad przetwarzaniem danych sprawuje Prezes UODO na podstawie ogólnych przepisów rozporządzenia 2016/679 (art. 32, art. 58), bez sektorowo dedykowanego mechanizmu certyfikacji dla oprogramowania medycznego.

3. Istniejące ramy prawne certyfikacji

Ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz.U. poz. 1017), obowiązująca od 28 sierpnia 2025 r., określa organizację krajowego systemu certyfikacji cyberbezpieczeństwa. Zgodnie z art. 2 pkt 2 tej ustawy certyfikacja oznacza potwierdzenie, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, osoba fizyczna lub system zarządzania cyberbezpieczeństwem spełniają wymogi określone w europejskim programie certyfikacji cyberbezpieczeństwa albo w krajowym schemacie certyfikacji cyberbezpieczeństwa. Zgodnie z art. 15 ust. 1 tej ustawy minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, krajowy schemat certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem lub osób fizycznych. Zakres upoważnienia obejmuje zatem produkty i usługi teleinformatyczne, a nie wyłącznie systemy zarządzania bezpieczeństwem. Instrument prawny pozwalający opisaną lukę usunąć obowiązuje zatem od 28 sierpnia 2025 r. — to jest na dziesięć miesięcy przed naruszeniem u dostawcy MyDr i dwanaście miesięcy przed naruszeniem w systemie Medyc. Brak jest nie podstawy ustawowej, lecz aktu wykonawczego obejmującego systemy teleinformatyczne służące prowadzeniu dokumentacji medycznej. Według stanu na dzień sporządzenia niniejszego wniosku na podstawie powołanej ustawy nie wydano żadnego rozporządzenia określającego krajowy schemat certyfikacji cyberbezpieczeństwa — dla jakiegokolwiek rodzaju produktów, usług, procesów ani systemów. Upoważnienie z art. 15 ust. 1 ustawy ma charakter fakultatywny i nie jest

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław

tel.: (71) 798-80-50 fax: (71) 798-80-51

e-mail: dil@dilnet.wroc.pl

obwarowane terminem; Izba nie podnosi zatem zarzutu uchybienia obowiązkom, lecz wskazuje, że przewidziany ustawą instrument pozostaje niewykorzystany, mimo że był dostępny przed oboma naruszeniami opisanymi w części II.

V. Instrumenty prawa unijnego i krajowego — zakres i terminy stosowania

1. Rozporządzenie (UE) 2025/327 (europejska przestrzeń danych zdrowotnych)

Rozporządzenie weszło w życie 26 marca 2025 r. i jest stosowane bezpośrednio, przy czym jego przepisy obowiązują etapami. Ustanawia obowiązkowy system oceny zgodności dla systemów elektronicznej dokumentacji zdrowotnej objętych jego zakresem, obejmujący dokumentację techniczną, deklarację zgodności UE, oznakowanie CE oraz wymagania w zakresie interoperacyjności, bezpieczeństwa i rejestrowania zdarzeń, wraz z obowiązkowymi komponentami harmonizacyjnymi. Dla sytuacji podmiotów wykonujących działalność leczniczą rozstrzygające są dwie okoliczności. Po pierwsze, obowiązki dotyczące zgodności tych systemów będą stosowane od 2029 r. dla pierwszej grupy kategorii danych (recepty elektroniczne i ich realizacja, skierowania, podstawowa informacja o pacjencie) oraz od 2031 r. dla kolejnej grupy (badania obrazowe, wyniki laboratoryjne, wypisy). Po drugie, ocena opiera się zasadniczo na ocenie dokonywanej przez producenta, nie na certyfikacji przez niezależną jednostkę. Deklaracja własna producenta nie dostarcza administratorowi danych niezależnego punktu odniesienia dla oceny wymaganej przez art. 28 ust. 1 rozporządzenia 2016/679 — również po 2029 r. Postulaty krajowe powinny być z tym reżimem zgodne i stanowić jego uzupełnienie w okresie przejściowym.

2. Rozporządzenie (UE) 2024/2847 (akt o cyberodporności)

Rozporządzenie ustanawia horyzontalne wymagania dla produktów z elementami cyfrowymi, obejmujące projektowanie zgodne z zasadami *secure by design* i *secure by default*, dokumentację techniczną, zarządzanie podatnościami oraz wykaz komponentów oprogramowania. Obowiązki zgłaszania aktywnie wykorzystywanych podatności i poważnych incydentów są stosowane od 11 września 2026 r., zasadnicza część pozostałych obowiązków — od 11 grudnia 2027 r. Zakres podmiotowy rozporządzenia nie jest automatyczny: usługa świadczona w modelu zdalnego przetwarzania nie zawsze stanowi produkt z elementami cyfrowymi, a produkty objęte reżimami sektorowymi mogą podlegać wyłączeniom lub szczególnemu traktowaniu. Naruszenia opisane w części II nastąpiły przed dniem rozpoczęcia stosowania obowiązków zgłoszeniowych. Niezależnie od tego Izba wskazuje lukę o charakterze praktycznym: nie istnieje kanał, którym informacja o podatności zgłoszonej na podstawie tego rozporządzenia dociera do podmiotów leczniczych korzystających z danego systemu. Obowiązek zgłoszenia został ustanowiony; przepływ informacji do podmiotu ponoszącego ryzyko — nie.

3. Ustawa o krajowym systemie cyberbezpieczeństwa

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. poz. 252), implementująca dyrektywę (UE) 2022/2555, weszła w życie 3 kwietnia 2026 r. Termin unijny transpozycji tej dyrektywy upłynął 17

października 2024 r. Dalszy harmonogram wdrożenia obejmuje termin wniosku o wpis do wykazu — 3 października 2026 r. — oraz termin wdrożenia obowiązków, w tym systemu zarządzania bezpieczeństwem informacji — 3 kwietnia 2027 r. Opóźnienie transpozycji zostało formalnie stwierdzone przez organ Unii. Komisja Europejska prowadziła wobec Rzeczypospolitej Polskiej postępowanie w sprawie uchybienia zobowiązaniom traktatowym: po upływie terminu transpozycji skierowała wezwanie do usunięcia uchybienia, a 7 maja 2025 r. wystosowała uzasadnioną opinię — do Polski i 18 innych państw członkowskich — z dwumiesięcznym terminem na odpowiedź, pod rygorem skierowania sprawy do Trybunału Sprawiedliwości Unii Europejskiej. Analogiczne postępowanie dotyczyło braku terminowej transpozycji dyrektywy (UE) 2022/2557. Naruszenia opisane w części II nastąpiły po wejściu nowelizacji w życie, lecz przed oboma terminami wdrożeniowymi. Przypisanie dostawcy systemu dokumentacji medycznej statusu podmiotu objętego ustawą wymaga odrębnej analizy jej definicji ustawowych; utrzymywanie systemu w infrastrukturze zewnętrznego dostawcy usług chmurowych nie czyni operatora tego systemu dostawcą usługi chmurowej. Izba zwraca natomiast uwagę na skutek czasowy opóźnienia: przesunęło ono o ponad siedemnaście miesięcy moment rozpoczęcia stosowania krajowych obowiązków implementujących dyrektywę (UE) 2022/2555 wobec podmiotów objętych zakresem nowelizacji. W okresie od 17 października 2024 r. do 3 kwietnia 2026 r. dostawcy nie podlegali obowiązkowi wynikającemu z krajowej implementacji tej dyrektywy — podlegali natomiast obowiązkowi adresowanemu bezpośrednio do podmiotów przetwarzających na podstawie rozporządzenia 2016/679, w szczególności art. 32. Brakowało nie obowiązku zapewnienia bezpieczeństwa, lecz skonkretyzowanego standardu sektorowego oraz mechanizmu uprzedniej weryfikacji jego dochowania.

4. Zalecenia CSIRT CeZ oraz pakiet „Cyber Piątka”

Dokument „Zalecenia bezpieczeństwa dla dostawców platform IT w ochronie zdrowia — w pigułce”, opracowany przez CSIRT CeZ we współpracy z Ministerstwem Zdrowia i przekazany dostawcom 16 września 2026 r., nie jest aktem prawnym. Stanowi listę kontrolną obejmującą zarządzanie bezpieczeństwem informacji i ocenę ryzyka, kontrolę dostępu i uwierzytelnianie wieloskładnikowe, zarządzanie uprawnieniami użytkowników, rejestrowanie i analizę zdarzeń, bezpieczeństwo interfejsów programistycznych, ochronę kopii zapasowych, kryptografię i zarządzanie kluczami oraz monitorowanie nietypowych wyszukiwań, pobrań i eksportów danych. Dokument nie tworzy obowiązków ani ich nie zastępuje. Przygotowywany pakiet legislacyjny określany jako „Cyber Piątka” zapowiada certyfikację podmiotów przetwarzających, standardy minimalne oraz podwyższone wymagania dla dostawców obsługujących powyżej 100 administratorów lub powyżej 100 tys. pacjentów. Izba zwraca uwagę na następstwo czasowe. Prace nad tym pakietem są **dopiero w toku**

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570
NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233
Legnica – pl. Słowiański 1, 59-220 Legnica
Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

— a zatem rozpoczęły się po naruszeniach opisanych w części II, nie przed nimi. Zapowiadane rozwiązania odpowiadają dokładnie tym brakom, które niniejszy wniosek opisuje: certyfikacji podmiotów przetwarzających, minimalnym standardom bezpieczeństwa oraz podwyższonym wymogom wobec największych dostawców. Okoliczność, że prawodawca uznaje je obecnie za potrzebne, jest potwierdzeniem, że w czasie, gdy doszło do naruszeń, mechanizmów tych nie było. Jednocześnie — dopóki pakiet nie zostanie uchwalony — skutki tego braku ponosi w całości podmiot wykonujący działalność leczniczą. To on jest adresatem roszczeń pacjentów (część II), na nim spoczywa ciężar dowodu odpowiedniości środków wdrożonych w infrastrukturze, do której nie ma dostępu (część VI.4), i to on ma samodzielnie określić wymagany poziom bezpieczeństwa, którego państwo dotąd nie zdefiniowało (część VI.1). Luka systemowa pozostaje zatem przeniesiona na administratora danych — stronę, która jej nie wywołała i nie miała narzucić, by jej zapobiec.

VI. Odpowiedzialność podmiotu wykonującego działalność leczniczą jako administratora danych

1. Treść obowiązku z art. 28 ust. 1 rozporządzenia 2016/679

Art. 28 ust. 1 rozporządzenia 2016/679 dopuszcza korzystanie wyłącznie z podmiotów przetwarzających zapewniających wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Treść tego pojęcia doprecyzowują Wytyczne Europejskiej Rady Ochrony Danych 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego. Waga tego dokumentu wynika z jego umocowania. Europejska Rada Ochrony Danych jest organem powołanym przez art. 68 rozporządzenia 2016/679, a wydawanie wytycznych wyjaśniających stosowanie rozporządzenia należy do jej zadań na podstawie art. 70 ust. 1 lit. e. W jej skład wchodzi przewodniczący krajowych organów nadzorczych — w przypadku Rzeczypospolitej Polskiej Prezes UODO. Wytyczne nie są prawnie wiążące i nie wiążą sądów ani Trybunału Sprawiedliwości Unii Europejskiej; stanowią natomiast istotny, instytucjonalnie umocowany instrument interpretacyjny służący jednolitemu stosowaniu rozporządzenia. Z Wytycznych wynikają cztery ustalenia istotne dla niniejszego wniosku. **Pkt 95 — wymóg wykazywalności.** Znaczenie mają gwarancje, które podmiot przetwarzający jest w stanie wykazać administratorowi, co zwykle wymaga wymiany dokumentacji: polityki bezpieczeństwa informacji, rejestru czynności przetwarzania, raportów audytów zewnętrznych, uznanych certyfikatów międzynarodowych. Katalog ten jest przykładowy. Ogólna deklaracja zgodności z rozporządzeniem, niepoparta żadnym elementem tego rodzaju, nie spełnia standardu, do którego się odwołuje.

Pkt 96 — proporcjonalność oceny. Ocena wystarczalności gwarancji stanowi formę oceny ryzyka, dokonywaną każdorazowo indywidualnie, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka dla praw i wolności osób fizycznych. Europejska Rada Ochrony Danych wskazuje wprost, że nie jest w stanie podać wyczerpującej listy wymaganych dokumentów ani działań, ponieważ zależy to od konkretnych okoliczności przetwarzania. Standard wymagany od

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

administratora jest zatem na gruncie samego rozporządzenia zdefiniowany jako proporcjonalny do jego sytuacji, nie jako audyt techniczny wymagany od każdego podmiotu niezależnie od skali działalności.

Pkt 97 — przedmiot oceny. Wiedza specjalistyczna, wiarygodność i zasoby podmiotu przetwarzającego, pomocniczo także jego reputacja rynkowa.

Pkt 99 — charakter ciągly. Obowiązek nie wyczerpuje się w chwili zawarcia umowy; administrator powinien w odpowiednich odstępach czasu weryfikować gwarancje podmiotu przetwarzającego. Rozporządzenie nie zwalnia administratora z tego obowiązku z powodu braku kompetencji technicznych. Trudność jest innej natury: informacje niezbędne do rzetelnej oceny — architektura systemów, procedury monitorowania, wyniki testów penetracyjnych — są chronione przez dostawców jako tajemnica przedsiębiorstwa i nie są udostępniane małym klientom na standardowych warunkach umów adhezyjnych. Realnym narzędziem pozostaje wówczas ocena treści umowy powierzenia pod kątem klauzul z art. 28 ust. 3 rozporządzenia, co stanowi warunek konieczny, lecz niewystarczający dla oceny wymaganej przez ust. 1.

2. Obowiązek informacyjny podmiotu przetwarzającego

Art. 28 ust. 3 lit. h rozporządzenia 2016/679 zobowiązuje podmiot przetwarzający do udostępnienia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w tym artykule oraz do umożliwiania audytów i przyczyniania się do nich. Jest to obowiązek podmiotu przetwarzającego, a nie uprawnienie uznaniowe dostawcy, i administrator może żądać jego wykonania niezależnie od tego, czy dysponuje kompetencjami do samodzielnego przeprowadzenia audytu technicznego. Rozróżnienie to ma znaczenie praktyczne. Prawo do audytu bez wzorca porównawczego jest w praktyce trudne do wykorzystania, ponieważ administrator nie ma punktu odniesienia dla oceny wyniku. Obowiązek informacyjny jest natomiast egzekwowalny i weryfikowalny. Zakres żądania musi być przy tym adekwatny i proporcjonalny, z uwzględnieniem ochrony tajemnicy przedsiębiorstwa oraz bezpieczeństwa pozostałych klientów dostawcy. Nieuzasadniona odmowa udostępnienia informacji niezbędnych do wykazania wykonania obowiązków z art. 28 rozporządzenia albo uniemożliwienie audytu może stanowić naruszenie art. 28 ust. 3 lit. h rozporządzenia. Izba zwraca przy tym uwagę, że certyfikaty systemów zarządzania (ISO/IEC 27001), raporty atestacyjne (SOC 2), audyty bezpieczeństwa oraz testy penetracyjne nie są mechanizmami certyfikacji w rozumieniu art. 42–43 rozporządzenia 2016/679. Stanowią wartościowy materiał dowodowy przy ocenie dostawcy, nie wywołując jednak skutków przewidzianych w rozporządzeniu dla certyfikacji zatwierdzonej.

3. Obowiązki z art. 24, 25 i 32 rozporządzenia 2016/679

Odpowiedzialność administratora nie wyczerpuje się w wyborze podmiotu przetwarzającego. Art. 24 rozporządzenia nakłada obowiązek wdrożenia odpowiednich środków z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz prawdopodobieństwa i wagi ryzyka. Art. 25 wymaga ochrony

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław

tel.: (71) 798-80-50 fax: (71) 798-80-51

e-mail: dil@dilnet.wroc.pl

danych w fazie projektowania oraz domyslniej ochrony danych. Art. 32 nakłada obowiązek zapewnienia bezpieczeństwa przetwarzania odpowiedniego do ryzyka, a ponieważ dane dotyczące zdrowia należą do szczególnych kategorii danych (art. 9 ust. 1), wymagany standard jest podwyższony. Obowiązki te obciążają podmiot leczniczy również w zakresie rozwiązania, którego nie projektuje i nad którym nie sprawuje kontroli technicznej. Art. 32 rozporządzenia adresuje przy tym obowiązki bezpośrednio także do podmiotu przetwarzającego, którego odpowiedzialność za bezpieczeństwo nie ogranicza się do zakresu wynikającego z umowy z administratorem.

4. Odpowiedzialność odszkodowawcza i rozkład ciężaru dowodu

Art. 82 ust. 2 rozporządzenia 2016/679 rozdziela przesłanki odpowiedzialności: administrator odpowiada za szkodę spowodowaną przetwarzaniem naruszającym rozporządzenie, a podmiot przetwarzający — gdy nie dopełnił obowiązków adresowanych bezpośrednio do podmiotów przetwarzających albo działał poza zgodnymi z prawem instrukcjami administratora lub wbrew nim. Odpowiedzialność solidarna z art. 82 ust. 4 powstaje, gdy oba podmioty odpowiadają za tę samą szkodę w tym samym przetwarzaniu; jej funkcją jest zapewnienie pełnego odszkodowania osobie, której dane dotyczą. Ryzyko podmiotu wykonującego działalność leczniczą jest przede wszystkim ryzykiem procesowym: może zostać pozwany i będzie zobowiązany wykazać przesłanki zwolnienia z art. 82 ust. 3 rozporządzenia, to jest że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody. Standard ten doprecyzował Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 14 grudnia 2023 r. w sprawie C-340/21 (*Natsionalna agentsia za prihodite*). Trybunał wskazał, że sam fakt dokonania naruszenia przez osobę trzecią nie wystarcza do przyjęcia, iż zastosowane środki techniczne i organizacyjne były nieodpowiednie, przy czym ciężar dowodu odpowiedzialności wdrożonych środków obciąża administratora, a okoliczność, że naruszenie zostało spowodowane przez sprawców przestępstwa, nie zwalnia go sama z siebie z odpowiedzialności. Dla małego podmiotu wykonującego działalność leczniczą obowiązek ten jest w części dotyczącej infrastruktury dostawcy istotnie utrudniony: wymaga wykazania odpowiedzialności środków wdrożonych w systemie, do którego podmiot ten nie ma i nie może mieć dostępu. W tym punkcie brak sektorowego mechanizmu niezależnej oceny przekłada się na sytuację procesową w/w podmiotu. Art. 82 rozporządzenia dotyczy odszkodowania za szkodę i nie stanowi podstawy obrony przed administracyjną karą pieniężną, nakazem organu nadzorczego, odpowiedzialnością zawodową ani roszczeniami z innych podstaw prawnych.

5. Standard należytej staranności

Przesłanki odpowiedzialności odszkodowawczej z art. 82 rozporządzenia 2016/679 mają charakter autonomiczny w prawie Unii i nie mogą być modyfikowane krajowym pojęciem należytej staranności. Trybunał Sprawiedliwości Unii Europejskiej wskazał, że samo naruszenie rozporządzenia nie wystarcza do przyznania odszkodowania,

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

konieczne jest wykazanie szkody oraz związku przyczynowego (wyrok z 4 maja 2023 r., C-300/21), że odpowiedzialność administratora opiera się na winie domniemanej, od której może się on uwolnić (wyrok z 11 kwietnia 2024 r., C-741/21), oraz że ciężar wykazania odpowiedzialności wdrożonych środków obciąża administratora (wyrok z 14 grudnia 2023 r., C-340/21). Art. 355 Kodeksu cywilnego może mieć w tym zakresie znaczenie pomocnicze przy ocenie zachowania administratora na gruncie prawa krajowego, o ile nie narusza treści i skuteczności art. 82 rozporządzenia. Zgodnie z art. 355 § 2 Kodeksu cywilnego należyta staranność w zakresie prowadzonej działalności gospodarczej określa się przy uwzględnieniu zawodowego charakteru tej działalności. Izba nie wywodzi z tego przepisu tezy, że bezpieczeństwo danych pozostaje poza zawodowym charakterem działalności leczniczej. Ochrona danych pacjentów jest elementem profesjonalnego wykonywania tej działalności. Zakres wymaganych działań powinien jednak uwzględniać skalę przedsiębiorstwa, poziom ryzyka oraz realne możliwości podmiotu — co jest zbieżne z zasadą proporcjonalności oceny wyrażoną w pkt 96 Wytycznych EROD 07/2020 i co Izba wnosi uczynić elementem stanowiska samorządu lekarskiego. Miarą nie może być standard dostępny wyspecjalizowanemu przedsiębiorstwu z własnym zespołem bezpieczeństwa informacji, lecz standard osiągalny dla podmiotu wykonującego działalność leczniczą danej skali.

6. Roszczenie zwrotne wobec dostawcy

Art. 82 ust. 5 rozporządzenia 2016/679 przyznaje podmiotowi, który wypłacił odszkodowanie w całości, prawo żądania od pozostałych uczestników przetwarzania zwrotu części odpowiadającej ich odpowiedzialności. Typowe postanowienia umów i regulaminów dostawców — limitujące odpowiedzialność kwotowo oraz zawężające ją do winy umyślnej lub rażącego niedbalstwa — mogą rodzić spór co do zakresu faktycznej rekompensaty. Odróżnić przy tym należy ustawowe roszczenie z art. 82 ust. 5 rozporządzenia od kontraktowych roszczeń odszkodowawczych i klauzul indemnifikacyjnych. Na gruncie prawa polskiego nieważne jest zastrzeżenie wyłączające odpowiedzialność za szkodę wyrządzoną umyślnie (art. 473 § 2 Kodeksu cywilnego). Istotne jest, że ograniczenie odpowiedzialności w relacji między dostawcą a podmiotem nie wywołuje skutków wobec pacjenta. Jeżeli administrator i podmiot przetwarzający ponoszą odpowiedzialność za tę samą szkodę, osoba, której dane dotyczą, może dochodzić pełnego odszkodowania od każdego z nich na zasadach art. 82 ust. 4 rozporządzenia; ograniczenie umowne administrator napotyka dopiero w relacji regresowej z dostawcą. Art. 28 ust. 10 rozporządzenia 2016/679 znajduje zastosowanie w sytuacji, w której podmiot przetwarzający, naruszając rozporządzenie, sam określa cele i sposoby przetwarzania, i wówczas jest uznawany za administratora w odniesieniu do tego przetwarzania. Niedostateczne zabezpieczenie danych, naruszenie art. 32 rozporządzenia lub działanie niezgodne z instrukcją administratora nie oznacza samo przez się, że podmiot przetwarzający określił cele i sposoby przetwarzania.

VII. Procedura postępowania na wypadek naruszenia u dostawcy

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław

tel.: (71) 798-80-50 fax: (71) 798-80-51

e-mail: dil@dilnet.wroc.pl

Podmiot wykonujący działalność leczniczą dotknięty potwierdzonym naruszeniem u swojego dostawcy staje przed wyborem między dalszym korzystaniem z systemu o podważonym bezpieczeństwie a ryzykiem zarzutu naruszenia obowiązku prowadzenia dokumentacji w postaci elektronicznej. W komunikatach Ministerstwa Zdrowia wskazywano, że przez brak warunków organizacyjno-technicznych w rozumieniu § 1 ust. 2 rozporządzenia z 6 kwietnia 2020 r. rozumie się zarówno trwały brak rozwiązań informatycznych, jak i ich czasową niemożność wykorzystania. Brak jest natomiast rozstrzygnięcia odniesionego do sytuacji następującej po naruszeniu bezpieczeństwa. Przesłanka ta ma charakter obiektywny i przejściowy. Należy odróżnić trzy stany faktyczne:

1. system jest niedostępny — stan najpełniej odpowiadający przesłance z § 1 ust. 2 rozporządzenia;
2. system jest technicznie dostępny, lecz został odłączony na czas analizy i zabezpieczenia incydentu — stan wymagający oceny z uwzględnieniem konieczności ochrony danych oraz zachowania ciągłości udzielania świadczeń;
3. system funkcjonuje, a podmiot leczniczy utracił do niego zaufanie — stan, który sam w sobie przesłanki tej nie wypełnia.

Przedmiotem wniosku nie jest uznanie wyjątku papierowego za uprawnienie do długotrwałej rezygnacji z dokumentacji elektronicznej. Przedmiotem wniosku jest ustalenie z góry, w którym z powyższych stanów i na jakich warunkach wyjątek znajduje zastosowanie, w jakim trybie podmiot leczniczy ma ten stan zgłosić oraz jakie są warunki powrotu do postaci elektronicznej. Czterokrotna nowelizacja rozporządzenia po ogłoszeniu tekstu jednolitego (Dz.U. z 2025 r. poz. 931 i 1853 oraz z 2026 r. poz. 758 i 876) nie objęła § 1 ust. 2 ani nie wprowadziła procedury postępowania na wypadek naruszenia u dostawcy. Konieczna jest procedura ciągłości działania ustalona zawczasu.

VIII. Wnioski

Dolnośląska Rada Lekarska we Wrocławiu wnosi, aby Naczelna Rada Lekarska podjęła stanowisko obejmujące następujące działania.

1. Wystąpienie o wprowadzenie obowiązkowej, niezależnej certyfikacji cyberbezpieczeństwa systemów teleinformatycznych służących prowadzeniu dokumentacji medycznej, opartej na wymogach określonych w akcie normatywnym.

Postulat obejmuje trzy nierozdzielne elementy.

1.1. Wymogi określone przez państwo. Minimalne wymogi bezpieczeństwa dla systemów służących prowadzeniu dokumentacji medycznej powinny zostać określone w akcie normatywnym, a ich zakres merytoryczny — oparty na dorobku już wypracowanym przez organy państwa, w szczególności na obszarach objętych zaleceniami CSIRT CeZ z 16 września 2026 r. (uwierzytelnianie wieloskładnikowe, zarządzanie uprawnieniami, bezpieczeństwo interfejsów programistycznych, ochrona

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

kopii zapasowych, kryptografia i zarządzanie kluczami, rejestrowanie zdarzeń, monitorowanie nietypowych pobrań i eksportów danych). Dokument ten ma dziś charakter wyłącznie zalecenia; jego treść jest natomiast gotowym punktem wyjścia dla wymogów wiążących.

1.2. Weryfikacja przez niezależną jednostkę. Ocena dochowania tych wymogów powinna być dokonywana przez akredytowaną jednostkę oceniającą zgodność, nie w trybie deklaracji własnej producenta. Jest to różnica rozstrzygająca dla sytuacji podmiotu leczniczego: deklaracja własna dostawcy nie dostarcza administratorowi niezależnego punktu odniesienia dla oceny wymaganej przez art. 28 ust. 1 rozporządzenia 2016/679, a właśnie na takim modelu oparte jest rozporządzenie (UE) 2025/327. Instrumentem właściwym jest krajowy schemat certyfikacji cyberbezpieczeństwa, który minister właściwy do spraw informatyzacji może określić w drodze rozporządzenia na podstawie art. 15 ust. 1 ustawy z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz.U. poz. 1017). Upoważnienie to obejmuje wprost produkty ICT, usługi ICT i procesy ICT, a art. 15 ust. 2 odnosi się odrębnie do rozporządzenia dotyczącego tych właśnie przedmiotów. Potwierdza to również art. 2 pkt 13 powołanej ustawy, odsyłający w pierwszym członie definicji do krajowego programu certyfikacji cyberbezpieczeństwa w rozumieniu art. 2 pkt 10 rozporządzenia (UE) 2019/881, którym jest zbiór reguł i procedur mających zastosowanie do certyfikacji lub oceny zgodności produktów ICT, usług ICT, procesów ICT albo usług zarządzanych w zakresie bezpieczeństwa. Ten element nie wymaga przeprowadzenia procesu legislacyjnego — wystarcza akt wykonawczy w ramach ustawy obowiązującej od 28 sierpnia 2025 r.

1.3. Obowiązkowy charakter certyfikacji. Izba wnosi, aby posiadanie certyfikatu stanowiło warunek dopuszczenia systemu do wykorzystania w celu prowadzenia dokumentacji medycznej przez usługodawców w rozumieniu ustawy o systemie informacji w ochronie zdrowia, w szczególności warunek podłączenia systemu do Systemu Informacji Medycznej. Certyfikacja dobrowolna nie usuwa bowiem zagadnienia będącego przedmiotem niniejszego wniosku. Podmiot wykonujący działalność leczniczą pozostaje zobowiązany do prowadzenia dokumentacji w postaci elektronicznej niezależnie od tego, czy jego dostawca zdecydował się poddać ocenie; możliwość wyboru dostawcy certyfikowanego istnieje tylko wtedy, gdy tacy dostawcy na rynku są. Instrument dobrowolny pozostawia zatem ryzyko tam, gdzie jest ono dziś — po stronie podmiotu o najmniejszych możliwościach jego oceny.

Obowiązkowy charakter certyfikacji jest prawnie dopuszczalny. Art. 56 ust. 2 rozporządzenia (UE) 2019/881 stanowi, że certyfikacja cyberbezpieczeństwa jest dobrowolna, **o ile prawo Unii lub prawo państwa członkowskiego nie stanowi inaczej** — a zatem wprost przewiduje możliwość ustanowienia obowiązku przez ustawodawcę krajowego. Ustawa z dnia 25 czerwca 2025 r. dostarcza schematu i trybu oceny; obowiązek posiadania certyfikatu wymaga odrębnej podstawy, której właściwym nośnikiem jest przygotowywany pakiet legislacyjny „Cyber Piątka” albo zmiana ustawy o systemie informacji w ochronie zdrowia. Powiązanie obowiązku z warunkami korzystania z Systemu Informacji Medycznej mieści się przy tym w

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

kompetencji państwa członkowskiego w zakresie organizacji i świadczenia opieki zdrowotnej (art. 168 ust. 7 Traktatu o funkcjonowaniu Unii Europejskiej).

1.4. Granice wynikające z prawa Unii. DIL wskazuje dwa ograniczenia, które projektowane rozwiązanie powinno respektować. Rozporządzenie (UE) 2025/327 harmonizuje wymagania dotyczące zharmonizowanych komponentów oprogramowania systemów elektronicznej dokumentacji zdrowotnej oraz przewiduje dla nich deklarację zgodności i oznakowanie CE. Wymóg krajowy nie powinien zatem ograniczać wprowadzania do obrotu systemów zgodnych z tym rozporządzeniem z powołaniem się na właściwości objęte harmonizacją, ani zastępować przewidzianej w nim oceny zgodności. Rozporządzenie to pozostawia natomiast państwom członkowskim kompetencję w zakresie wymogów dotyczących komponentów innych niż zharmonizowane oraz warunków podłączania świadczeniodawców do krajowych infrastruktur, przy czym spełnienie tych warunków może podlegać ocenie przez niezależną jednostkę na poziomie krajowym. Na tej właśnie kompetencji opiera się postulat z pkt 1.3. Zgodnie z art. 57 rozporządzenia (UE) 2019/881 krajowe programy certyfikacji dla produktów, usług i procesów ICT objętych przyjętym europejskim programem certyfikacji przestają wywoływać skutki na zasadach określonych w tym przepisie. Schemat krajowy powinien być zatem stosowany w zakresie nieobjętym programem europejskim i ustąpić mu w razie jego przyjęcia dla tej kategorii systemów, przy zachowaniu ważności certyfikatów już wydanych. Przed wydaniem rozporządzenia zasadne jest zbadanie, czy i w jakim zakresie oprogramowanie tego rodzaju może być objęte europejskim programem EUCC (rozporządzenie wykonawcze Komisji (UE) 2024/482), którego metodyka oparta na kryteriach Common Criteria adresowana jest przede wszystkim do produktów o przeznaczeniu horyzontalnym.

2. Wystąpienie do Ministra Zdrowia o określenie procedury ciągłości działania dla podmiotów wykonujących działalność leczniczą dotkniętych naruszeniem ochrony danych u dostawcy — przez wydanie oficjalnego stanowiska co do zastosowania § 1 ust. 2 rozporządzenia z dnia 6 kwietnia 2020 r. w trzech stanach faktycznych wyodrębnionych w części VII albo przez odpowiednią zmianę rozporządzenia określającą dopuszczalny czas prowadzenia dokumentacji w postaci papierowej, tryb zgłoszenia oraz warunki powrotu do postaci elektronicznej. Ponieważ stanowisko Ministra nie wiąże sądów ani organów nadzorczych, Izba wnosi o dążenie do uzgodnionego stanowiska Ministerstwa Zdrowia, Centrum e-Zdrowia, Prezesa UODO oraz CSIRT CeZ, a docelowo do zmiany przepisu.

3. Podjęcie inicjatywy opracowania sektorowego kodeksu postępowania w rozumieniu art. 40 rozporządzenia 2016/679 dla dostawców systemów dokumentacji medycznej, zatwierdzanego przez Prezesa UODO, wraz z mechanizmem monitorowania zgodności z art. 41 rozporządzenia oraz sektorowych kryteriów certyfikacji na podstawie art. 42–43 rozporządzenia. Izba zwraca uwagę, że certyfikacja przewidziana w art. 42–43 rozporządzenia 2016/679 dotyczy operacji przetwarzania wykonywanych przez administratorów i podmioty przetwarzające, nie zaś oceny produktu informatycznego jako takiego; postulat dotyczy zatem

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, lp., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

certyfikacji określonych operacji przetwarzania realizowanych przez dostawców. DIL wnosi przy tym o taki kształt postulatu, który uwzględnia art. 42 ust. 4 rozporządzenia 2016/679, zgodnie z którym certyfikacja nie zmniejsza odpowiedzialności administratora ani podmiotu przetwarzającego za zgodność z rozporządzeniem. Zatwierdzony kodeks postępowania oraz certyfikacja powinny być zatem postulowane jako istotny materiał dowodowy przy ocenie wykonania obowiązków z art. 24, 28 i 32 rozporządzenia oraz jako okoliczność uwzględniana przy wymiarze administracyjnej kary pieniężnej na podstawie art. 83 ust. 2 lit. j rozporządzenia, bez ingerencji w zasady odpowiedzialności odszkodowawczej z art. 82.

4. Postulat ustanowienia kanału przekazywania podmiotom wykonującym działalność leczniczą informacji o podatnościach i poważnych incydentach zgłaszanych przez dostawców na podstawie rozporządzenia (UE) 2024/2847, z rolą pośredniczącą Centrum e-Zdrowia.

5. Wystąpienie do Prezesa UODO o wydanie zaleceń sektorowych określających przykładowy, proporcjonalny zakres weryfikacji gwarancji dostawcy oraz sposób jej dokumentowania przez podmiot leczniczy o skali małego przedsiębiorcy, z odniesieniem do zasady proporcjonalności oceny wyrażonej w pkt 96 Wytycznych EROD 07/2020. Z uwagi na indywidualny, oparty na ryzyku charakter obowiązku z art. 28 ust. 1 rozporządzenia 2016/679 Izba nie wnosi o ustanowienie zamkniętego katalogu czynności zwalniającego z odpowiedzialności.

6. Opracowanie i udostępnienie członkom izb lekarskich pakietu narzędzi praktycznych, obejmującego:

- wzorec wniosku do dostawcy o udostępnienie informacji na podstawie art. 28 ust. 3 lit. h rozporządzenia 2016/679, wraz z zestawem pytań kontrolnych opartym na obszarach objętych zaleceniami CSIRT CeZ;
- wzorec umowy powierzenia przetwarzania danych z katalogiem klauzul rekomendowanych i niedopuszczalnych, w szczególności dotyczących granic kwotowego ograniczenia odpowiedzialności dostawcy;
- wzorec notatki z okresowego przeglądu gwarancji dostawcy, dokumentującej wykonanie ciągłego obowiązku z art. 28 ust. 1 rozporządzenia.

Narzędzia te wyrównują pozycję negocjacyjną pojedynczej praktyki wobec umowy adhezyjnej dużego dostawcy oraz umożliwiają członkom izb udokumentowanie należytej staranności przed wystąpieniem incydentu.

IX. Uzasadnienie pilności

1. Ryzyko zmaterializowało się dwukrotnie w ciągu jednego kwartału 2026 r., u dwóch niezależnych dostawców.
2. Pierwsze postępowania sądowe toczą się przeciwko placówkom medycznym, nie przeciwko dostawcom systemów.
3. Okres przejściowy jest długi i obciąża w/w podmioty. Obowiązki wynikające z nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa stają się wymagalne 3 kwietnia 2027 r., zasadnicza część obowiązków z rozporządzenia (UE) 2024/2847 — 11 grudnia 2027 r., a ocena zgodności systemów na podstawie rozporządzenia (UE)

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław
tel.: (71) 798-80-50 fax: (71) 798-80-51
e-mail: dil@dilnet.wroc.pl

2025/327 — od 2029 i 2031 r. W całym tym okresie odpowiedzialność wobec pacjenta pozostaje po stronie podmiotu leczniczego w niezmiennym kształcie.

4. Prace nad pakietem legislacyjnym „Cyber Piątka” są dopiero w toku. Rozpoczęły się one po naruszeniach opisanych w części II, a zapowiadane w nich rozwiązania — certyfikacja podmiotów przetwarzających i minimalne standardy bezpieczeństwa — odpowiadają brakom, których skutki w okresie poprzedzającym ponosił i nadal ponosi podmiot leczniczy. Etap prac legislacyjnych stwarza przy tym sposobność przedstawienia stanowiska samorządu lekarskiego przed przyjęciem rozwiązań.

5. Element postulatu określony w pkt VIII.1.2 — ustanowienie schematu certyfikacji — może zostać zrealizowany aktem wykonawczym w ramach ustawy obowiązującej od 28 sierpnia 2025 r., bez konieczności przeprowadzenia procesu legislacyjnego. Instrument ten był dostępny przed oboma naruszeniami opisanymi w części II i do dnia sporządzenia niniejszego wniosku nie został wykorzystany w odniesieniu do żadnego rodzaju produktów, usług ani systemów. Nadanie certyfikacji charakteru obowiązkowego (pkt VIII.1.3) wymaga odrębnej podstawy ustawowej, dla której naturalnym nośnikiem jest pakiet legislacyjny będący obecnie w przygotowaniu.

X. Podsumowanie

1. Dysproporcja między możliwościami a oczekiwaniami.

Określenie wymaganego poziomu bezpieczeństwa systemów przetwarzających dane szczególnej kategorii wymaga kompetencji, zasobów i aparatu, którymi państwo dysponuje: wyspecjalizowanych służb cyberbezpieczeństwa, zespołu reagowania na incydenty działającego w Centrum e-Zdrowia, organu nadzorczego, krajowego systemu akredytacji oraz możliwości wydania aktu normatywnego. Adresatem obowiązku zdefiniowania i zweryfikowania tego poziomu jest natomiast — poprzez otwarte pojęcie „wystarczających gwarancji” z art. 28 ust. 1 rozporządzenia 2016/679 — indywidualna praktyka lekarska, nierzadko jednoosobowa działalność gospodarcza, nieposiadająca ani komórki informatycznej, ani prawnej. Jest to dysproporcja nie stopnia, lecz rodzaju: oczekuje się wykonania zadania od strony, która nie ma do niego narzędzi, podczas gdy strona je posiadająca pozostawiła je nieużyte.

2. **Opóźnienie po stronie definiowania standardów.** Termin transpozycji dyrektywy (UE) 2022/2555 upłynął 17 października 2024 r., a nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa weszła w życie 3 kwietnia 2026 r. Opóźnienie zostało formalnie stwierdzone przez Komisję Europejską w uzasadnionej opinii z 7 maja 2025 r. Niezależnie od tego instrument pozwalający ustanowić krajowy schemat certyfikacji istnieje od 28 sierpnia 2025 r. i do dziś nie został wykorzystany wobec żadnej kategorii produktów, usług ani systemów. Opóźnienie dotyczyło zatem tej czynności, której od administratora oczekuje się nieprzerwanie: ustalenia, jaki poziom zabezpieczeń jest wymagany.

3. **Skutki ponosi administrator.** Pierwsze powództwa zostały skierowane przeciwko trzem placówkom medycznym, nie przeciwko dostawcy systemu. Ciężar dowodu odpowiedniości wdrożonych środków obciąża administratora (wyrok TSUE z 14

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogńskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław

tel.: (71) 798-80-50 fax: (71) 798-80-51

e-mail: dil@dilnet.wroc.pl

grudnia 2023 r., C-340/21), również w zakresie infrastruktury, do której nie ma i nie może mieć dostępu. Skutki braku, którego administrator nie wywołał i któremu nie mógł zapobiec, przenoszą się więc na niego — w postępowaniu cywilnym i w ocenie nadzorczej.

4. Pakiet „Cyber Piątka” jako potwierdzenie istnienia luki. Prace nad pakietem zapowiadającym certyfikację podmiotów przetwarzających, minimalne standardy bezpieczeństwa oraz podwyższone wymogi wobec największych dostawców trwają obecnie — a zatem rozpoczęły się po naruszeniach opisanych w części II. Prawodawca nie tworzy nowych ram obowiązkowych dla obszarów już wystarczająco uregulowanych. Przystąpienie do prac nad takimi rozwiązaniami jest w ocenie Izby stanowiskiem prawodawcy przyznającym — po fakcie — że mechanizmów tych wcześniej nie było. Wniosek, który z tego wynika, dotyczy nie odpowiedzialności za przeszłość, lecz rozkładu obowiązków na przyszłość: skoro brak mechanizmu został uznany, nie można jednocześnie utrzymywać, że jego skutki miał ponosić podmiot, który żadnego mechanizmu ustanowić nie mógł. Z tych powodów Dolnośląska Rada Lekarska wnosi jak w części VIII.

Załącznik — wykaz powołanych przepisów, orzeczeń i dokumentów Prawo Unii Europejskiej

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (ogólne rozporządzenie o ochronie danych): art. 9 ust. 1, art. 24, art. 25, art. 28 ust. 1, ust. 3 lit. h, ust. 5 i ust. 10, art. 32, art. 40, art. 41, art. 42 (w tym ust. 4), art. 43, art. 58, art. 68, art. 70 ust. 1 lit. e, art. 82 ust. 2–5, art. 83 ust. 2 lit. j
- Rozporządzenie (UE) 2017/745 w sprawie wyrobów medycznych: art. 2 pkt 1, załącznik VIII (reguła 11)
- Rozporządzenie (UE) 2019/881 (akt o cyberbezpieczeństwie): art. 2 pkt 10, art. 56 ust. 2, art. 57
- Rozporządzenie wykonawcze Komisji (UE) 2024/482 (europejski program certyfikacji EUCC)
- Rozporządzenie (UE) 2024/2847 (akt o cyberodporności)
- Rozporządzenie (UE) 2025/327 w sprawie europejskiej przestrzeni danych zdrowotnych
- Traktat o funkcjonowaniu Unii Europejskiej: art. 168 ust. 7
- Dyrektywa (UE) 2022/2555 (NIS2)
- Dyrektywa (UE) 2022/2557 (CER)

Prawo polskie

- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2026 r. poz. 208): art. 2 pkt 6, art. 11 ust. 1 i 1b, art. 13a, art. 56 ust. 2a i ust. 4
- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta: art. 30 ust. 1

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych



Dolnośląska Izba Lekarska we Wrocławiu

ul. Kazimierza Wielkiego 45, 50-077 Wrocław

tel.: (71) 798-80-50 fax: (71) 798-80-51

e-mail: dil@dilnet.wroc.pl

- Ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz.U. poz. 1017): art. 1, art. 2 pkt 2, pkt 12 i pkt 13, art. 6 ust. 1 i 2, art. 15 ust. 1–4
- Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. poz. 252)
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20)
- Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2024 r. poz. 798, z 2025 r. poz. 931 i 1853 oraz z 2026 r. poz. 758 i 876): § 1 ust. 1 i ust. 2
- Kodeks cywilny: art. 355 § 1 i § 2, art. 473 § 2

Orzecznictwo

- Wyrok TSUE z dnia 4 maja 2023 r. w sprawie C-300/21, *UI przeciwko Österreichische Post AG*
- Wyrok TSUE z dnia 14 grudnia 2023 r. w sprawie C-340/21, *Natsionalna agentsia za prihodite*
- Wyrok TSUE z dnia 11 kwietnia 2024 r. w sprawie C-741/21, *juris GmbH*

Dokumenty organów i instytucji

- Wytyczne Europejskiej Rady Ochrony Danych 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego w RODO, pkt 94–99
- Wytyczne MDCG 2019-11 w sprawie kwalifikacji i klasyfikacji oprogramowania
- Uzasadniona opinia Komisji Europejskiej z dnia 7 maja 2025 r. w sprawie braku zgłoszenia pełnej transpozycji dyrektywy (UE) 2022/2555
- CSIRT CeZ, *Zalecenia bezpieczeństwa dla dostawców platform IT w ochronie zdrowia — w pigułce*, 16 września 2026 r.

Źródła prasowe

- K. Nocuń, *Dane medyczne a prywatna firma: co z nadzorem, certyfikacją? Centrum e-Zdrowia odpowiada*, Rynek Zdrowia, 14 sierpnia 2026 r.
- money.pl, wrzesień 2026 r. — informacja o powództwach przeciwko placówkom medycznym

z poważaniem

Przewodnicząca
Komisji Legislacyjnej DRL
Marzena Kufel
lek. dent. Marzena Kufel

Prezes
Dolnośląskiej Rady Lekarskiej
dr n.med. Wojciech Florjański

Konto: PKO BP 62 1020 5242 0000 2402 0349 0570

NIP: 896-10-01-140

Delegatury:

Jelenia Góra – Szpital Wojewódzki, ul. Ogińskiego 6, 58-506 Jelenia Góra, Ip., pok. 233

Legnica – pl. Słowiański 1, 59-220 Legnica

Wałbrzych – ul. Moniuszki 1/1, 58-300 Wałbrzych

