

Pytania do dostawcy oprogramowania medycznego

W sierpniu 2026 wyciekły dane pacjentów z systemu dokumentacji medycznej, z którego korzystały tysiące placówek. Zgłoszenia do UODO i zawiadomienia pacjentów spadły na placówki, bo to one są administratorami danych, a dostawca był podmiotem przetwarzającym. Do 17 września do Prezesa UODO wpłynęło ponad 2 tys. zawiadomień od administratorów. Formularz zamienia zalecenia CSIRT CeZ dla dostawców na pytania, na które dostawca odpowiada na piśmie.

12.08.2026

UODO: zawiadomienie pacjentów to obowiązek administratorów, czyli placówek

16.09.2026

zalecenia CSIRT CeZ dla dostawców platform IT w ochronie zdrowia

do końca 2026

dodatkowe kontrole UODO w zakresie danych o zdrowiu

3.04.2027

koniec okresu dostosowawczego KSC, w tym łańcuch dostaw

Wyślijcie formularz osobno do dostawcy każdego systemu z danymi pacjentów: szpitalnego (HIS), przychodni lub gabinetu, laboratorium (LIS), diagnostyki obrazowej (RIS i PACS), rejestracji internetowej. Opis „Czego oczekujemy” pod pytaniem to minimum, z którym placówka wykaże, że korzysta z dostawcy dającego wystarczające gwarancje (art. 28 ust. 1 RODO) i sama umie wykazać zgodność (art. 5 ust. 2 RODO). Kratkę zaznacza placówka po przeczytaniu odpowiedzi i tylko wtedy, gdy dostawca dołączył dowód. „Spełniamy RODO” bez dokumentu liczy się jako brak. Dłuższą odpowiedź dostawca dołącza jako załącznik z numerem pytania. Gdy system pracuje na serwerach placówki, pytania 8, 12, 13 i 14 dotyczą też waszego działu IT: dostawca opisuje, co system umożliwia, a placówka, jak to skonfigurowała.

Placówka

System i wersja

Dostawca, osoba odpowiadająca

Data wystania, termin odpowiedzi

UMOWA I ROLA Kto odpowiada za dane

- ☐ **1. Na podstawie jakiej umowy przetwarzacie dane naszych pacjentów i czy zawiera ona wszystko, czego wymaga RODO?**

Czego oczekujemy: umowa powierzenia z elementami art. 28 ust. 3 lit. a do h RODO, w tym pomocą przy obowiązkach z art. 32 do 36 i prawem placówki do audytu; tajemnica informacji o pacjencie, także po jego śmierci (art. 24 ust. 6 ustawy o prawach pacjenta). Dowód: aktualna umowa.

Odpowiedź dostawcy

- ☐ **2. Z jakich podwykonawców korzystacie przy naszych danych (serwery, chmura, kopie, wsparcie, usługi sztucznej inteligencji) i w jakich krajach są dane?**

Czego oczekujemy: wykaz z rolą i krajem przetwarzania; informacja o każdej planowanej zmianie z możliwością sprzeciwu (art. 28 ust. 2 i 4 RODO); przekazanie poza EOG tylko na warunkach rozdziału V RODO (art. 44); dane nie służą do trenowania modeli ani innym celom dostawcy bez polecenia placówki (art. 28 ust. 3 lit. a RODO). Dowód: wykaz podwykonawców.

Odpowiedź dostawcy

- ☐ **3. W jakim czasie, jakim kanałem i z jakimi informacjami powiadomicie nas o naruszeniu lub incydencie po waszej stronie?**

Czego oczekujemy: czas w godzinach w umowie, kontakt całodobowy, potwierdzenie, czy incydent dotyczy naszych danych, i dane do zgłoszenia: charakter naruszenia, liczba osób, skutki, podjęte środki (art. 33 ust. 2 i 3 RODO). Placówka zgłasza naruszenie Prezesowi UODO w miarę możliwości w 72 godziny od stwierdzenia (art. 33 ust. 1 RODO), a podmiot kluczowy lub ważny przekazuje wczesne ostrzeżenie o incydencie poważnym w 24 godziny od wykrycia (art. 11 ust. 1 pkt 4 ustawy o KSC). Dowód: zapis w umowie.

Odpowiedź dostawcy

TOŻSAMOŚĆ I DOSTĘP Kto wchodzi do systemu

- ☐ **4. Czy logowanie wieloskładnikowe jest wymuszone dla kont administracyjnych, serwisowych i dostępu spoza sieci placówki? Czy możemy je włączyć wszystkim użytkownikom?**

Czego oczekujemy: tak dla kont uprzywilejowanych, metodą odporną na wyłudzenie, na przykład kluczem sprzętowym albo kartą z certyfikatem (kod SMS takiej odporności nie daje); możliwość włączenia dla wszystkich (CSIRT CeZ). Dowód: opis konfiguracji.

Odpowiedź dostawcy

☐ 5. Którzy wasi pracownicy mają dostęp do naszej bazy produkcyjnej, na jakich kontaktach i kto ten dostęp włącza? Czy kopie naszej bazy trafiają do środowisk testowych? Czego oczekujemy: konta imienne, bez wspólnych kont serwisowych; dostęp czasowy, włączany na zgłoszenie i rejestrowany; w testach dane zanonimizowane albo spseudonimizowane (CSIRT CeZ); upoważnienie placówki jako administratora (art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta). Dowód: lista osób, wpis w dzienniku dostępu.	Odpowiedź dostawcy
☐ 6. Jak system ogranicza uprawnienia naszych użytkowników? Czego oczekujemy: role sprawdzane po stronie serwera, a nie tylko ukryte przyciski; raport uprawnień do przeglądu; blokada nieużywanych kont (CSIRT CeZ); dostęp do dokumentacji wyłącznie dla uprawnionych (§ 1 ust. 4 pkt 1 rozporządzenia w sprawie dokumentacji medycznej). Dowód: raport uprawnień.	Odpowiedź dostawcy

INTERFEJSY I INTEGRACJE Którędy dane wychodzą z systemu

☐ 7. Jakie interfejsy API udostępnia system (aplikacja pacjenta, rejestracja internetowa, P1, laboratoria, inne systemy) i jak są chronione? Czego oczekujemy: wykaz interfejsów; uwierzytelnianie i autoryzacja każdego wywołania, limity zapytań, walidacja; osobna tożsamość i rotacja poświadczeń dla każdej integracji, sekrety poza kodem (CSIRT CeZ). Dowód: wykaz i wynik ostatniego testu bezpieczeństwa API.	Odpowiedź dostawcy
☐ 8. Czy nasze dane leżą na infrastrukturze wspólnej z innymi klientami, a jeśli tak, jak są oddzielone? Czego oczekujemy: izolacja wymuszona w warstwie serwerowej i w bazie, testy prób dostępu między klientami, całodobowy monitoring (CSIRT CeZ, systemy obsługujące wiele podmiotów). Dowód: opis architektury i wynik testu.	Odpowiedź dostawcy
☐ 9. Jak szybko w razie incydentu zablokujecie konta, unieważnicie poświadczenia i odetniecie integrację? Kto o tym decyduje? Czego oczekujemy: procedura z rolami, kontaktami i czasem w godzinach, zabezpieczenie dowodów (CSIRT CeZ); uzgodnione, kto w placówce zgadza się na odcięcie, bo odcięta integracja zatrzymuje rejestrację albo laboratorium. Dowód: procedura obsługi incydentu.	Odpowiedź dostawcy

REJESTROWANIE I EKSPORT Kto co odczytał i co wyniósł

☐ 10. Czy system zapisuje, kto, kiedy, skąd i co odczytał, zmienił lub wyeksportował? Gdzie są te zapisy, jak długo i czy mamy do nich wgląd? Czego oczekujemy: rejestr logowań, zmian uprawnień, dostępu administracyjnego, odczytów i eksportów, trzymany poza produkcją i chroniony przed usunięciem (CSIRT CeZ); osoba i czas każdej zmiany w dokumentacji (§ 1 ust. 6 pkt 3 i 4 rozporządzenia w sprawie dokumentacji medycznej); okres przechowywania w umowie. Dowód: raport dostępu do danych jednego pacjenta.	Odpowiedź dostawcy
☐ 11. Jak wykrywacie masowe odczyty i eksporty danych, także rozłożone na wiele dni, i co się wtedy dzieje? Czego oczekujemy: limity i dodatkowe potwierdzenie dla operacji wysokiego ryzyka, na przykład eksportu całej bazy pacjentów; wykrywanie anomalii w API i wyprowadzania danych rozłożonego w czasie; alarm z przypisaną osobą (CSIRT CeZ). Dowód: opis reguł i przykład alarmu.	Odpowiedź dostawcy

SZYFROWANIE, KOPIE, OTWARZANIE Co zostaje po ataku

☐ 12. Czy dane są szyfrowane w transmisji, w bazie i w kopiach? Gdzie są klucze? Czego oczekujemy: szyfrowanie uznanymi metodami we wszystkich trzech miejscach; klucze oddzielnie od danych, z rotacją i procedurą unieważnienia (CSIRT CeZ); szyfrowanie jako środek z art. 32 ust. 1 lit. a RODO). Dowód: opis metod i miejsca kluczy.	Odpowiedź dostawcy
☐ 13. Gdzie są kopie naszych danych i czy przynajmniej jedna przetrwa przejście środowiska produkcyjnego? Czego oczekujemy: kopie szyfrowane i odseparowane od produkcji, co najmniej jedna niezmienna albo poza siecią, osobne konta do zarządzania kopiami (CSIRT CeZ); zdolność szybkiego przywrócenia dostępu do danych (art. 32 ust. 1 lit. c RODO). Dowód: schemat kopii.	Odpowiedź dostawcy
☐ 14. Kiedy ostatnio odtworzyliście system z kopii, w jakim scenariuszu i ile to trwało? Czego oczekujemy: protokół z datą, czasem odtworzenia i utratą danych, także dla ataku szyfrującego i utraty kluczy; czas odtworzenia (RTO) i dopuszczalna utrata danych (RPO) w umowie (CSIRT CeZ; regularne testowanie, art. 32 ust. 1 lit. d RODO). Dowód: protokół z ostatnich 12 miesięcy.	Odpowiedź dostawcy

WYTWARZANIE I NADZÓR Jak dostawca pilnuje samego siebie

☐ 15. Czy macie system zarządzania bezpieczeństwem informacji, kto go niezależnie sprawdził i w jakim czasie usuwacie krytyczne podatności?

Czego oczekujemy: system oparty na ISO/IEC 27001 i niezależny audyt; certyfikat, jeśli jest, obejmujący ten system, nie tylko biuro; czas usunięcia podatności krytycznej w umowie; wykaz komponentów oprogramowania, czyli SBOM (CSIRT CeZ). Podmiot kluczowy lub ważny ocenia podatności i jakość produktów dostawcy w ramach łańcucha dostaw (art. 8 ust. 1 pkt 2 lit. e i ust. 2 ustawy o KSC). Dowód: certyfikat z zakresem, data testu penetracyjnego.

Odpowiedź dostawcy

☐ 16. Kto u was odpowiada za wdrożenie zaleceń CSIRT CeZ z 16.09.2026 i jaki jest status każdego z nich?

Czego oczekujemy: tabela zaleceń z właścicielem, statusem i terminem, potwierdzona dokumentacją konfiguracji, wynikami testów lub logami (CSIRT CeZ, weryfikacja realizacji zaleceń). Dowód: tabela statusu.

Odpowiedź dostawcy

KONIEC WSPÓŁPRACY Jak odzyskamy dane

☐ 17. Jak przekażecie nam komplet danych przy zakończeniu umowy i co stanie się z kopiami?

Czego oczekujemy: eksport całości danych w standardach pozwalających odtworzyć je w innym systemie (§ 1 ust. 6 pkt 8 rozporządzenia w sprawie dokumentacji medycznej); zwrot albo usunięcie danych i kopii według decyzji placówki (art. 28 ust. 3 lit. g RODO); przekazanie placówce danych z dokumentacji (art. 24 ust. 7 ustawy o prawach pacjenta). Dokumentację przechowuje się co do zasady 20 lat (art. 29 ust. 1 tej ustawy). Dowód: próbny eksport.

Odpowiedź dostawcy

Z PRAKTYKI Typowe błędy przy ocenie dostawcy

- Umowa powierzenia na wzorzec dostawcy, bez czasu powiadomienia w godzinach. Przy incydencie 72 godziny placówki biegają, a dostawca „informuje bez zbędnej zwłoki”.
- Jedno konto serwisowe dostawcy, wspólne dla kilku osób i włączone na stałe. Po incydencie nie da się ustalić, kto się logował.
- Kopia w tej samej chmurze i na tym samym koncie co produkcja. Kto przejmie produkcję, usunie też kopię.
- Brak wglądu w dziennik odczytów i eksportów. Po wycieku placówka nie wie, czyje dane wyszły, i zawiadamia wszystkich pacjentów.
- Pytania trafiają tylko do dostawcy głównego systemu, a laboratorium, diagnostyka obrazowa i rejestracja internetowa, które mają te same dane, zostają bez nich.

WYNIK: POLICZ KRATKI ZAZNACZONE Z DOWODEM (NA 17)

15 do 17	Dołączcie odpowiedzi do rejestru czynności przetwarzania (art. 30 RODO) i do dokumentacji bezpieczeństwa. Powtórzcie pytania po każdej większej zmianie systemu.
9 do 14	Braki w pytaniach 3, 5, 13 i 14 wpiszcie do aneksu z terminem. Od nich zależy, czy po incydencie zdążycie w 72 godziny i czy będzie z czego odtworzyć dane.
0 do 8	Umówcie spotkanie z dostawcą z udziałem inspektora ochrony danych i przygotujcie aneks. Zamawiający publiczny w następnym postępowaniu wpisuje wymagania do opisu przedmiotu zamówienia (art. 99 Pzp) albo sprawdza rynek we wstępnych konsultacjach (art. 84 Pzp).

Skala ma znaczenie. Gabinet i przychodnia zatrudniające mniej niż 50 osób zwykle nie są podmiotem kluczowym ani ważnym według ustawy o KSC (art. 5), ale RODO i ustawa o prawach pacjenta obowiązują je w całości; zacznijcie od pytań 1, 3, 4, 13 i 17. Samodzielny publiczny zakład opieki zdrowotnej jest podmiotem ważnym przy zatrudnieniu od 50 do 249 osób, a kluczowym od 250 (art. 5 ust. 8 ustawy o KSC); szpital w formie spółki ocenia się według progów dla średniego przedsiębiorcy (art. 5 ust. 1 pkt 1 i ust. 2 pkt 1). Taki szpital pyta każdego dostawcę systemu z danymi pacjentów i dołącza odpowiedzi do oceny ryzyka łańcucha dostaw, a kierownik odpowiada także za obowiązki powierzone innej osobie (art. 8c ust. 3). Sieć placówek zbiera odpowiedzi raz dla wszystkich lokalizacji i prowadzi jeden rejestr dostawców, ale umowę powierzenia zawiera każdy podmiot, który jest administratorem danych.

Kwestia Skali, blog Arkadiusza Łobodźca o IT w ochronie zdrowia. Formularz ma charakter pomocniczy i nie zastępuje analizy prawnej ani audytu; zalecenia CSIRT CeZ nie są przepisem prawa. Podstawy: RODO, rozporządzenie (UE) 2016/679; ustawa o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2026 r. poz. 20 ze zm., w tym poz. 252; ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta, Dz.U. z 2024 r. poz. 581 ze zm.; rozporządzenie Ministra Zdrowia w sprawie dokumentacji medycznej, Dz.U. z 2024 r. poz. 798 ze zm.; Prawo zamówień publicznych, Dz.U. z 2026 r. poz. 793. Stan prawny na 28.09.2026. Wydawca: OneCare sp. z o.o., ul. Pokrzywy 4, 05-850 Kręćki, NIP 1182322364, KRS 0001221324. Pytania: arkadiusz.lobodziec@kwestiaskali.pl. Wersja 1.2.