

# Gotowość szpitala na KSC do 3 kwietnia 2027

Wpis do wykazu podmiotów kluczowych i ważnych sam niczego w szpitalu nie zabezpiecza. Ta lista sprawdza, czy obowiązki z ustawy o krajowym systemie cyberbezpieczeństwa działają w praktyce. Punkty ułożyliśmy w kolejności, w jakiej warto je robić przez sześć miesięcy, które zostały do końca okresu dostosowawczego.

**3.10.2026**

koniec samorejestracji w wykazie

**3.04.2027**

koniec okresu dostosowawczego: obowiązki wdrożone, korzystanie z systemu S46

**3.04.2028**

termin pierwszego audytu bezpieczeństwa systemu informacyjnego podmiotu kluczowego

**3.04.2028**

od tego dnia można nakładać kary pieniężne, także na kierownika podmiotu

Zaznacz punkt tylko wtedy, gdy macie dowód: dokument, zapis, protokół albo wynik testu. „Mamy, ale nie spisaliśmy” liczy się jako brak. Terminy według Ministerstwa Cyfryzacji (gov.pl, najważniejsze terminy nowelizacji KSC) i przepisów przejściowych ustawy z 23.01.2026 o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026 poz. 252, art. 33 i 35). Terminy dotyczą placówek, które spełniały przesłanki podmiotu kluczowego albo ważnego 3.04.2026, w dniu wejścia nowelizacji w życie. „Ustawa o KSC” w przypisach to ustawa z 5.07.2018 o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20 ze zm.).

## PAŹDZIERNIK

### Spis tego, co mamy

- ☐ **Mamy aktualny spis systemów, serwerów i stacji roboczych z przypisanym właścicielem każdego systemu.**

Dowód: rejestr zasobów z datą ostatniej aktualizacji.

Podstawa: art. 8 ust. 1 pkt 2 lit. m ustawy o KSC (zarządzanie aktywami).

- ☐ **Wiemy, które urządzenia medyczne są podłączone do sieci, jaki mają system i kto je serwisuje.**

Dowód: lista urządzeń uzgodniona między działem IT a działem aparatury.

- ☐ **Mamy listę dostawców z dostępem zdalnym: kto, do czego, jakim kontem i od kiedy.**

Dowód: rejestr dostępów zdalnych; żadne konto serwisowe nie jest wspólne dla kilku osób.

- ☐ **Sprawdziliśmy, czy placówka jest w wykazie podmiotów kluczowych i ważnych, a jeśli powinna być, a nie jest, zarejestrowaliśmy ją.**

Dowód: potwierdzenie wpisu w wykazie.

Podstawa: art. 7c ust. 1 ustawy o KSC i art. 33 ust. 3 ustawy nowelizującej (Dz.U. 2026 poz. 252); termin 3.10.2026 z harmonogramu Ministra Cyfryzacji.

## LISTOPAD

### Ryzyko i kopie zapasowe

- ☐ **Dla każdego krytycznego systemu (szpitalny, laboratorium, diagnostyka obrazowa, apteka) wiemy, jak długo szpital może działać bez niego.**

Dowód: analiza ryzyka z określonym czasem odtworzenia i dopuszczalną utratą danych.

Podstawa: art. 8 ust. 1 pkt 1 ustawy o KSC.

- 
- ☐ **Kopie zapasowe są w co najmniej jednym miejscu, którego nie da się skasować ani zaszyfrować z poziomu sieci szpitala.**  
Dowód: opis konfiguracji kopii i miejsca ich przechowywania.
  - ☐ **W ostatnich sześciu miesiącach odtworzyliśmy co najmniej jeden krytyczny system z kopii na osobnym serwerze albo w wydzielonym środowisku.**  
Dowód: protokół testu z datą, osobą i czasem odtworzenia.  
**Podstawa:** art. 8 ust. 1 pkt 2 lit. f ustawy o KSC; art. 32 ust. 1 lit. c i d RODO. Przepisy nie podają częstotliwości testu; sześć miesięcy to nasza praktyka.
  - ☐ **Sieć z urządzeniami medycznymi i systemami klinicznymi jest oddzielona od sieci administracyjnej i sieci dla gości.**  
Dowód: schemat sieci i reguły ruchu między segmentami.
- 

## GRUDZIEŃ

### Incydent i praca bez systemu

- ☐ **Procedura incydentu mówi, kto decyduje o zgłoszeniu incydentu poważnego i kto je wysyła: wczesne ostrzeżenie w 24 godziny od wykrycia, zgłoszenie w 72 godziny od wykrycia, sprawozdanie końcowe w miesiąc od zgłoszenia.**  
Dowód: procedura z nazwiskami i zastępstwami, znana dyżurom.  
**Podstawa:** art. 11 ust. 1 pkt 4, 4a i 4c ustawy o KSC; zgłoszenia idą przez system S46 (art. 11 ust. 2).
  - ☐ **Izba przyjęć, apteka i laboratorium mają spisany sposób pracy, gdy system szpitalny nie działa.**  
Dowód: procedura awaryjna i wydrukowane formularze w miejscu pracy.
  - ☐ **Każdy incydent, także drobny albo zgłoszony przez pacjenta, trafia do rejestru z przyczyną i wnioskami.**  
Dowód: rejestr incydentów z ostatnich miesięcy; na stronie internetowej placówki informacja o cyberzagrożeniach i sposób zgłoszenia incydentu.  
**Podstawa:** art. 11 ust. 1 pkt 1 i art. 2 pkt 10 ustawy o KSC (obsługa incydentu obejmuje jego rejestrowanie); art. 9 ust. 1 pkt 2 i 3 ustawy o KSC (wiedza o cyberzagrożeniach i możliwość zgłoszenia incydentu dla użytkownika usługi; wiedzę można udostępnić odnośnikiem do stron CSIRT, art. 9 ust. 4).
  - ☐ **Wiemy, jak zgłosić naruszenie ochrony danych osobowych Prezesowi UODO w 72 godziny od jego stwierdzenia i kiedy trzeba zawiadomić pacjentów.**  
Dowód: procedura naruszenia ochrony danych uzgodniona z inspektorem ochrony danych.  
**Podstawa:** art. 33 ust. 1 RODO (zgłoszenie organowi nadzorczemu); art. 34 ust. 1 RODO (zawiadomienie osób, gdy naruszenie może powodować wysokie ryzyko).
- 

## STYCZEŃ

### System zarządzania bezpieczeństwem

- ☐ **Polityka bezpieczeństwa opisuje szpital taki, jaki jest dziś, na podstawie spisu, analizy ryzyka i testów.**  
Dowód: dokument zatwierdzony przez kierownika, z datą przeglądu.  
**Podstawa:** art. 8 ust. 1 pkt 2 lit. a, art. 8d pkt 1 i art. 10 ust. 1 ustawy o KSC.

- 
- ☐ **Uprawnienia nadaje się według ról, osoby z zadaniami z cyberbezpieczeństwa dopuszcza się do pracy po przedstawieniu informacji z Krajowego Rejestru Karnego, a konto osoby, która odchodzi, jest wyłączone w ciągu doby.**

Dowód: procedura, przykład z ostatniego odejścia pracownika, informacje z KRK w aktach osób z zadaniami z cyberbezpieczeństwa.

Podstawa: art. 8 ust. 1 pkt 2 lit. n ustawy o KSC (polityki kontroli dostępu); art. 8f ust. 1 ustawy o KSC (informacja o niekaralności za przestępstwa przeciwko ochronie informacji od osób realizujących zadania z art. 8 lub 11). Termin jednej doby to nasza praktyka, nie wymóg przepisu.

---

- ☐ **Konta administracyjne i dostęp zdalny wymagają drugiego składnika logowania.**

Dowód: konfiguracja dla kont administracyjnych, VPN i dostępu dostawców.

Podstawa: art. 8 ust. 1 pkt 2 lit. l ustawy o KSC (uwierzytelnianie wieloskładnikowe w stosownych przypadkach).

---

- ☐ **Aktualizacje systemów mają ustalony rytm i właściciela, a wyjątki (np. urządzenia medyczne bez aktualizacji) są opisane.**

Dowód: harmonogram aktualizacji i rejestr wyjątków.

Podstawa: art. 8 ust. 1 pkt 5 lit. b ustawy o KSC.

---

## LUTY

### Dostawcy

- ☐ **Zapytaliśmy dostawców oprogramowania medycznego, jak stosują zalecenia CSIRT CeZ przekazane dostawcom 16.09.2026 (ezdrowie.gov.pl): logowanie wieloskładnikowe, bezpieczeństwo interfejsów, ochrona kopii, kryptografia, monitorowanie eksportów danych.**

Dowód: odpowiedzi dostawców na piśmie.

Podstawa: art. 8 ust. 1 pkt 2 lit. e i art. 8 ust. 2 ustawy o KSC (łańcuch dostaw). Zalecenia CSIRT CeZ same nie są przepisem; datę przekazania podaje komunikat UODO z 25.09.2026 (uodo.gov.pl).

---

- ☐ **Umowy z kluczowymi dostawcami mówią, w jakim czasie dostawca zgłasza szpitalowi incydent po swojej stronie.**

Dowód: zapis w umowie albo aneks.

Podstawa: art. 8 ust. 1 pkt 2 lit. e ustawy o KSC; art. 33 ust. 2 RODO (podmiot przetwarzający zgłasza naruszenie administratorowi bez zbędnej zwłoki).

---

- ☐ **Wiemy, gdzie dostawcy przetwarzają dane pacjentów i czy korzystają z podwykonawców.**

Dowód: umowy powierzenia z listą podwykonawców i lokalizacją danych.

Podstawa: art. 28 ust. 2 i 3 RODO.

---

- ☐ **Dane szpitala da się wyeksportować w standardowym formacie, a dostęp do danych jest kontrolowany i rejestrowany.**

Dowód: opis eksportu i dziennik dostępu do danych w systemie.

---

## MARZEC

### Ludzie i próba

- ☐ **Kierownik podmiotu i osoba, której powierzył obowiązki w zakresie cyberbezpieczeństwa, przeszli w tym roku kalendarzowym szkolenie z obowiązków wynikających z ustawy i wiedzą, że powierzenie zadań nie zdejmuje odpowiedzialności z kierownika.**

Dowód: lista obecności i materiał szkolenia.

Podstawa: art. 8e ust. 1 i 3 oraz art. 8c ust. 1 i 3 ustawy o KSC.

- ☐ **Personel z dostępem do systemów przeszedł szkolenie z rozpoznawania podejrzanych wiadomości i zgłaszania incydentów.**

Dowód: rejestr szkoleń.

Podstawa: art. 8 ust. 1 pkt 2 lit. i oraz art. 8d pkt 4 ustawy o KSC.

- ☐ **Korzystamy z systemu S46, wyznaczaliśmy osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa i sprawdziliśmy, kto i jak korzysta z S46.**

Dowód: dokument wyznaczenia osób do kontaktu; dostęp do S46 osób wskazanych w procedurze incydentu.

Podstawa: art. 9 ust. 1 pkt 1 ustawy o KSC (co najmniej dwie osoby; wyjątki dla mikro i małych przedsiębiorców oraz podmiotów ważnych będących podmiotami publicznymi w art. 9 ust. 2 i 3); art. 9 ust. 1 pkt 4 i art. 11 ust. 2 ustawy o KSC.

- ☐ **Przeprowadziliśmy ćwiczenie przy stole: atak w piątek po południu, przy stole dyrekcja, IT, pielęgniarka naczelna, izba przyjęć i dostawca systemu.**

Dowód: notatka z ćwiczenia z listą luk i terminami poprawek.

Podstawa: art. 8 ust. 1 pkt 2 lit. f ustawy o KSC (testowanie planów ciągłości działania i planów awaryjnych).

**WYNIK: POLICZ PUNKTY ZAZNACZONE Z DOWODEM (NA 24)**

**20 do 24** Obowiązki działają. Utrzymujcie rytm: przegląd i test odtworzenia co pół roku.

**12 do 19** Fundamenty są, luki też. Zaczynjcie od punktów z listopada i grudnia, bo to one decydują o skutkach ataku.

**0 do 11** Do kwietnia 2027 trzeba przejść cały plan. Zaczynjcie od spisu i testu kopii, dokumenty zostawcie na koniec.

**Skala ma znaczenie.** Szpital powiatowy z małym działem IT nie musi budować własnego centrum monitorowania; może kupić je jako usługę, jeśli umowa mówi, kto co robi w pierwszej godzinie incydentu. Szpital specjalistyczny musi dodatkowo zapanować nad urządzeniami medycznymi w sieci. Sieć szpitali może zrobić spis, procedury i wymagania wobec dostawców raz dla wszystkich lokalizacji, ale każdy podmiot wpisany do wykazu ma własnego kierownika i ustala, kto zgłasza incydent w jego imieniu. Przychodnia, która nie jest podmiotem kluczowym ani ważnym, nie ma obowiązków z ustawy o KSC, ale punkty o kopiach, umowach powierzenia i naruszeniu ochrony danych dotyczą jej tak samo, bo wynikają z RODO. Więcej: kwestiaskali.pl.

**Kwestia Skali**, blog Arkadiusza Łobodźca o IT w ochronie zdrowia. Lista ma charakter pomocniczy i nie zastępuje analizy prawnej ani audytu. Stan prawny na 28.09.2026. Wydawca: OneCare sp. z o.o., ul. Pokrzywy 4, 05-850 Kręczki, NIP 1182322364, KRS 0001221324. Pytania: [arkadiusz.lobodziec@kwestiaskali.pl](mailto:arkadiusz.lobodziec@kwestiaskali.pl). Wersja 2.2.