NIS2 / ustawa o KSC / Cyber Resilience Act

NIS2 i znowelizowana ustawa o krajowym systemie cyberbezpieczeństwa (KSC, w mocy od 3 kwietnia 2026 r.) nakładają obowiązki na firmy uznane za podmioty kluczowe lub ważne. Program nie „zapewnia zgodności" sam w sobie – pomaga ją wykazać w obszarach, których dotyczy. Poniżej zestawienie: wymaganie art. 21 ust. 2 dyrektywy NIS2, co robi OpiekunDB i co pozostaje po stronie Twojej organizacji.

WYMAGANIE (ART. 21 UST. 2 NIS2)	OPIEKUNDB	ORGANIZACJA KLIENTA
`lit. c` **Ciągłość działania, kopie zapasowe, odtwarzanie po awarii** Program to zapewnia	• Kopie pełne, różnicowe i dziennika transakcji baz SQL Server według planu (także Express), kopie folderów. • Kopia w repozytorium poza firmą (Warszawa, UE) i lokalnie na serwerze. • Kopie niezmienne przez 30 dni (Object Lock, tryb Compliance) – odporne na ransomware i przejęte hasła. • Serwer zapasowy z aktualnymi bazami – przełączenie planowe bez utraty danych, po awarii w kilka minut. • Pakiet awaryjny i kod odzyskiwania z wydrukowanego arkusza – odtworzenie konfiguracji na nowym serwerze.	• Plan ciągłości działania i plan odtwarzania (kto, co, w jakiej kolejności). • Okresowe próbne odtworzenie i zapis jego wyniku.
`lit. f` **Ocena skuteczności środków bezpieczeństwa** Program to zapewnia	• Każda kopia sprawdzana – RESTORE VERIFYONLY, sumy kontrolne, test rozpakowania archiwum. • Kontrola spójności baz (DBCC CHECKDB) w harmonogramie. • Raport dzienny lub tygodniowy e-mailem i alarm, gdy problem trwa – historia do pokazania audytorowi. • Serwer zapasowy odtwarza każdą kopię – stały, faktyczny test odtwarzalności.	• Przegląd raportów i reakcja na alarmy; włączenie wyników do przeglądu skuteczności SZBI.
`lit. h` **Kryptografia i szyfrowanie** Program to zapewnia	• Szyfrowanie AES-256 na Twoim serwerze, zanim kopia opuści firmę; przesył wyłącznie HTTPS. • Hasła szyfrowania tylko u Ciebie – dostawca nie zna haseł i nie może odczytać kopii. • Sekrety zapisane w systemie Windows (DPAPI), hasło administratora PBKDF2.	• Polityka kryptograficzna organizacji, przechowywanie arkusza odzyskiwania i pakietu awaryjnego.
`lit. i` **Kontrola dostępu i rozliczalność** Program to zapewnia	• Hasło administratora chroni zmiany ustawień, zatrzymanie usługi i odtworzenie z zastąpieniem bazy. • Dziennik zmian – kto (użytkownik Windows), kiedy i z którego komputera zmienił konfigurację lub się logował. • Wpisy połączone sumami kontrolnymi (wykrycie zmiany lub usunięcia), kopia co godzinę w repozytorium z blokadą zmian.	• Nadawanie i odbieranie dostępu do serwera i konfiguratora, przegląd dziennika zmian.

WYMAGANIE (ART. 21 UST. 2 NIS2)	OPIEKUNDB	ORGANIZACJA KLIENTA
`lit. d` **Bezpieczeństwo łańcucha dostaw** Program pomaga	• Instalator i aktualizacje podpisane certyfikatem; program sprawdza podpis przed instalacją. • Repozytorium w centrum danych w Polsce; podmiot przetwarzający wskazany w umowie powierzenia. • Ta karta, regulamin i umowa powierzenia jako materiał do oceny dostawcy.	• Ocena dostawców i ryzyka łańcucha dostaw w ramach własnego SZBI.
`lit. e` **Utrzymanie systemów i obsługa podatności** Program pomaga	• Automatyczne aktualizacje w nocy z kopią konfiguracji przed instalacją; aktualizacje bezpieczeństwa zawsze. • Zgłaszanie podatności i ich obsługa – zasady na stronie Bezpieczeństwo (zgodnie z CRA).	• Aktualizacje systemu Windows i SQL Server na serwerze.
`lit. b` **Obsługa incydentów** Program pomaga	• Alarmy e-mailem o braku kopii, braku sygnału z serwera, próbie nadpisania kopii w repozytorium. • Dziennik zdarzeń i dziennik zmian jako materiał do analizy incydentu.	• Procedura obsługi incydentów i zgłoszenia do CSIRT (24 h / 72 h / 1 miesiąc).
`lit. j` **Uwierzytelnianie wieloskładnikowe** Po stronie organizacji	• Program nie ma dziś własnego MFA (planowane jako opcja).	• MFA na poziomie dostępu do serwera (RDP, VPN, logowanie do Windows) – obejmuje także konfigurator.
`lit. a, g` **Analiza ryzyka, polityki, szkolenia, cyberhigiena** Po stronie organizacji	• Poza zakresem programu.	• Należą do Twojej organizacji (SZBI do 3 kwietnia 2027 r. dla podmiotów objętych ustawą o KSC).

Cyber Resilience Act (rozporządzenie UE 2024/2847)

OpiekunDB jest produktem z elementami cyfrowymi w rozumieniu CRA. Od 11 września 2026 r. producent zgłasza aktywnie wykorzystywane podatności i poważne incydenty dotyczące produktu do CSIRT i ENISA. Podatności można zgłaszać na adres kontakt@opiekundb.pl (temat „PODATNOŚĆ") – zasady na stronie Bezpieczeństwo. Pełne wymagania CRA (m.in. deklaracja zgodności i oznakowanie CE) obowiązują od 11 grudnia 2027 r.

Karta ma charakter informacyjny i nie stanowi opinii prawnej. O tym, czy Twoja organizacja jest podmiotem kluczowym lub ważnym, decydują przepisy ustawy o KSC. Aktualna wersja karty: https://opiekundb.pl/nis2/ · kontakt: kontakt@opiekundb.pl