NIS 2 ART. 21(2)(D)

Kwestionariusz dla dostawców NIS 2

Otwarty, zakotwiczony w prawie UE kwestionariusz do oceny dostawców w ramach NIS 2

Profil dostawcy	18 pól
Praktyki bezpieczeństwa	26 pól
Specyficzne dla SaaS	5 pól
Specyficzne dla On-Premise	4 pól
Professional Services	3 pól
Managed Services	3 pól

Każde pole jest zakotwiczone w pierwotnym źródle na poziomie UE: NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, GDPR Art. 28 lub Cyber Resilience Act. Uzupełnienia sektorowe (TISAX, VDA ISA, BSI C5, KRITIS) są dodawane do tej podstawy.

Źródło: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

OPEN SOURCE
NISD2.eu
www.nisd2.eu

Licencja: MIT (schemat) + CC BY 4.0 (treść). Można swobodnie używać, forkować i adaptować.

1. Profil dostawcy

18 pól

Nazwa prawna

STRING · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2

Zarejestrowana nazwa Twojej firmy, taka jak widnieje w rejestrze handlowym. Przykład: Müller GmbH lub Acme Software Ltd.

Adres siedziby

STRING · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2

Zarejestrowany adres prowadzenia działalności Twojej firmy. Wystarczy jeden adres, nawet jeśli masz kilka lokalizacji.

Kraj

COUNTRY · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2

Kraj, w którym Twoja firma ma siedzibę prawną. Dwie litery, np. DE dla Niemiec.

Domena główna

URL · OPCJONALNE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Twoja domena główna, zwykle adres URL Twojej witryny. Przykład: acmesoftware.com.

Slogan (jedna linia, widoczny dla klientów)

STRING · OPCJONALNE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Jedna linia podsumowująca Twoją ofertę. Klienci widzą ją w Twoim profilu dostawcy. Przykład: ERP dla produkcji w sektorze MŚP.

Opis publiczny (dłuższy)

TEXT · OPCJONALNE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Dwa do trzech zdań o Twojej firmie i tym, czym się zajmuje. Pojawia się to w Twoim profilu dostawcy. Argumentacja sprzedażowa, postawa w zakresie bezpieczeństwa lub oba elementy.

Opis świadczonych usług

TEXT · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2(B) + §5.1.4 TIPS

Jeden akapit o tym, co Twoja firma technicznie dostarcza klientom. Konkretne produkty, moduły lub usługi. Unikaj czysto marketingowego języka.

Kraje / regiony, w których przetwarzane są dane klientów

STRING · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.4 TIPS

Wszystkie kraje, w których przechowywane lub przetwarzane są dane Twoich klientów. Oddzielone przecinkami, kody krajów ISO. Przykład: DE, NL, US. Jeśli przetwarzasz dane wyłącznie w UE, wystarczy wymienić kraje UE.

Imię i nazwisko kontaktu ds. bezpieczeństwa

STRING · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(D)

Osoba, z którą klienci kontaktują się w przypadku incydentu bezpieczeństwa. W mniejszych firmach często dyrektor zarządzający lub kierownik IT. Wystarczy jedna osoba.

E-mail kontaktowy do zgłaszania incydentów

EMAIL · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(D)

Adres e-mail, którego klienci używają do zgłaszania incydentu bezpieczeństwa. Najlepiej lista dystrybucyjna, taka jak security@example.com, która dociera do wielu osób.

Telefon kontaktowy do zgłaszania incydentów (24/7)

PHONE · OPCJONALNE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(D)

Numer telefonu do pilnych zgłoszeń incydentów. Jeśli nie prowadzisz dyżuru 24/7, podaj godziny pracy w nawiasie.

SLA powiadamiania o incydentach (godziny)

INTEGER · OPCJONALNE · PODSTAWA PRAWNA: NIS2 ART. 23

Liczba godzin od wykrycia incydentu do powiadomienia klienta, najpóźniej. Realistyczna samoocena, a nie wartość docelowa. Typowe wartości: 24, 48 lub 72 godziny.

Identyfikator rejestracji BSI (tylko jeśli Twoja firma sama podlega NIS2)

STRING · OPCJONALNE · PODSTAWA PRAWNA: ENISA TIG §5.1.2

Jeśli Twoja firma sama podlega NIS 2 i jest zarejestrowana w BSI, wpisz tutaj identyfikator rejestracji. Opcjonalne. Pozwala klientom od razu zobaczyć, że spełniasz ten sam obowiązek co podmiot regulowany.

Świadczymy usługi SaaS / hostowane

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Uruchamiasz oprogramowanie dla klientów na własnej infrastrukturze i dostarczasz je przez internet. Zaznacz więcej niż jedno pole, jeśli oferujesz kilka modeli.

Dostarczamy oprogramowanie on-premise

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Dostarczasz oprogramowanie, które klienci instalują i uruchamiają na własnej infrastrukturze.

Świadczymy usługi profesjonalne / doradztwo

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Twoim głównym produktem jest praca ludzka: doradztwo, wdrożenie, szkolenia, audyt lub dostosowanie.

Świadczymy usługi zarządzane / MSP

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.2(B)

Obsługujesz dla klienta części jego infrastruktury IT, własnym personelem. Typowe dla modeli MSP i MSSP.

Używamy, integrujemy lub dostarczamy systemy SI

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(D)

Czy Twoje produkty lub usługi przetwarzają dane klientów za pomocą modelu SI lub ML? Obejmuje to modele zewnętrzne wywoływane przez API, na przykład OpenAI lub Anthropic.

2. Praktyki bezpieczeństwa

26 pól

Udokumentowany system zarządzania bezpieczeństwem informacji (ISMS)

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.2(A)

Zaznacz tak, jeśli masz pisemną politykę bezpieczeństwa informacji z przypisanymi rolami, regularnymi przeglądami i udokumentowaną obsługą incydentów. Certyfikacja ISO 27001 lub BSI Grundschutz oznacza tak.

Posiadanie certyfikatu ISO 27001, BSI Grundschutz lub równoważnego

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.2(B)

Zaznacz tak, jeśli Twoja firma posiada aktualnie certyfikat ISO 27001, BSI Grundschutz, SOC 2 Type II lub równoważny. Prześlij certyfikat w zakładce Certyfikaty.

Coroczne szkolenie z zakresu świadomości bezpieczeństwa dla całego personelu

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(B)

Zaznacz tak, jeśli każdy pracownik otrzymuje co najmniej jedno coroczne szkolenie z zakresu świadomości bezpieczeństwa informacji. E-learning się liczy; symulacje phishingu są uzupełnieniem.

Weryfikacja przeszłości personelu z dostępem do danych klientów

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(C)

Zaznacz tak, jeśli przeprowadzasz weryfikację przeszłości personelu z dostępem do danych klientów. Typowy poziom: wyciąg z rejestru karnego lub równoważny dokument przy zatrudnieniu.

Udokumentowany proces obsługi podatności i instalowania poprawek

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(F)

Zaznacz tak, jeśli masz pisemny proces obsługi podatności bezpieczeństwa: wykrywanie, ocena, priorytetyzacja, instalowanie poprawek lub łagodzenie. Monitorowanie CVE i instalowanie poprawek w oparciu o SLA są standardem.

Akceptacja prawa klienta do audytu (lub udostępnianie raportów z audytu)

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(E)

Zaznacz tak, jeśli przyznajesz klientom prawo do audytu na miejscu albo udostępniasz zastępcze raporty z audytu (na przykład SOC 2, ISAE 3402).

Korzystanie z podwykonawców przetwarzania / poddostawców

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(G)

Zaznacz tak, jeśli do świadczenia usługi korzystasz z innych firm, które mają dostęp do danych lub infrastruktury klientów. Typowe przykłady: AWS, Azure, Cloudflare, Stripe.

Lista podwykonawców przetwarzania

TEXT · WARUNKOWE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(G)

Wymień każdego podwykonawcę przetwarzania z nazwą, miejscem przetwarzania i tym, co dla Ciebie robi. Wystarczy tabela lub lista punktowana. Aktualizuj ją za każdym razem, gdy dodajesz lub usuwasz podwykonawcę.

Zobowiązanie do zwrotu / zniszczenia danych klientów po zakończeniu umowy

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(H)

Zaznacz tak, jeśli zobowiązujesz się umownie do zwrotu lub zniszczenia danych klientów po zakończeniu umowy. Powszechna praktyka: eksport i zwrot, a następnie usunięcie w ciągu 30 dni.

Dostępna standardowa umowa o przetwarzaniu danych (DPA)

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: GDPR ART. 28

Zaznacz tak, jeśli masz standardową umowę o przetwarzaniu danych zgodnie z artykułem 28 GDPR, którą klienci mogą podpisać. Wymagane, gdy tylko przetwarzasz dane osobowe.

Polityki bezpieczeństwa są przeglądane co najmniej raz w roku

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(A) / ENISA TIG §1.1

Zaznacz tak, jeśli Twoje polityki bezpieczeństwa są przeglądane co najmniej raz w roku i aktualizowane w razie potrzeby. Pisemna notatka w dokumencie jest wystarczającym dowodem.

Udokumentowany plan reagowania na incydenty

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(B) / ENISA TIG §3

Zaznacz tak, jeśli masz pisemny plan obsługi incydentów bezpieczeństwa: kto decyduje, kto komunikuje, kto dokumentuje. Co najmniej jedno ćwiczenie sztabowe rocznie to dobra praktyka.

Udokumentowany plan ciągłości działania / odtwarzania po awarii

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(C) / ENISA TIG §4

Zaznacz tak, jeśli masz plan wyjaśniający, jak utrzymujesz działanie lub szybko przywracasz je podczas awarii: systemy krytyczne, rozwiązania awaryjne, cele RTO i RPO.

Udokumentowana polityka kryptografii

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Zaznacz tak, jeśli masz pisemnie określone, jaką kryptografię stosujesz i gdzie: dane w tranzycie (TLS 1.2+), dane w spoczynku (AES-256), zarządzanie kluczami, algorytmy haszujące.

Zarządzanie dostępem uprzywilejowanym (PAM) dla personelu wewnętrznego

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Zaznacz tak, jeśli administratorzy i konta uprzywilejowane mają dodatkowe mechanizmy kontroli: osobne logowanie, MFA, rejestrowanie sesji lub dostęp just-in-time.

MFA wymuszone dla wszystkich wewnętrznych kont administracyjnych / uprzywilejowanych

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(J)

Zaznacz tak, jeśli każde wewnętrzne konto administracyjne lub uprzywilejowane musi używać MFA. Tokeny sprzętowe lub aplikacje uwierzytelniające się liczą; SMS nie.

Prowadzenie inwentaryzacji zasobów informacyjnych

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(I) / ENISA TIG §12.4

Zaznacz tak, jeśli prowadzisz aktualną listę każdego systemu informacyjnego używanego do świadczenia usługi: serwery, bazy danych, narzędzia SaaS, punkty końcowe. Wystarczy arkusz kalkulacyjny.

Program testów penetracyjnych co rok lub co dwa lata

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(E) / ENISA TIG §6.5

Zaznacz tak, jeśli zlecasz zewnętrzny test penetracyjny co najmniej raz na jeden do dwóch lat. W przypadku mniejszych firm akceptowalnym minimalnym krokiem jest zewnętrzne skanowanie podatności.

Ujawniamy przeszłe podlegające zgłoszeniu zdarzenia cyberbezpieczeństwa na prośbę klientów

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.2

Zaznacz tak, jeśli na prośbę klienta otwarcie ujawniasz, czy i jakie podlegające zgłoszeniu incydenty bezpieczeństwa Twoja firma miała w przeszłości. Typowy okres: ostatnie od trzech do pięciu lat.

Zapewniamy klientom pomoc w razie incydentu bez kosztów / po kosztach ustalonych z góry

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.4 TIPS

Zaznacz tak, jeśli zobowiązujesz się pomagać klientom bez dodatkowych kosztów, gdy incydent jest spowodowany przez Twój produkt lub usługę. Jeśli zamiast tego z góry uzgadniasz wcześniej zdefiniowaną stawkę dzienną, również zaznacz tak.

Pełna współpraca z właściwymi organami (BSI, ENISA, krajowe CSIRT)

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.4 TIPS

Zaznacz tak, jeśli zobowiązujesz się do pełnej współpracy z właściwymi organami, takimi jak BSI, ENISA lub krajowe CSIRT, podczas inspekcji, audytów i obsługi incydentów. Standard dla poważnych dostawców.

Powiadamiamy klientów o każdej istotnej zmianie wpływającej na świadczenie usługi

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.4 TIPS

Zaznacz tak, jeśli zobowiązujesz się powiadamiać klientów o każdej istotnej zmianie wpływającej na Twoją zdolność do świadczenia usługi: przejęcia, zmiany podwykonawcy przetwarzania, poważne zmiany techniczne.

Powiadamiamy klientów z wyprzedzeniem, jeśli zmieniają się miejsca przetwarzania danych

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.4 TIPS

Zaznacz tak, jeśli informujesz klientów z wyprzedzeniem, zanim zmieni się miejsce przetwarzania ich danych. Ważne dla ochrony danych i dla zgodnego z GDPR nadzoru nad łańcuchem dostaw.

Udokumentowana strategia wyjścia z obowiązkowym okresem przejściowym

BOOLEAN · WYMAGANE · PODSTAWA PRAWNA: ENISA TIG §5.1.4 TIPS

Zaznacz tak, jeśli masz pisemną strategię wyjścia: jak długo trwa uporządkowane przekazanie, jakie dane i wiedza są przekazywane, do czego się zobowiązujesz w okresie przejściowym.

Dostarczamy SBOM-for-AI zgodnie z minimalnymi elementami G7

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(D) / ENISA TIG §5.1.2

Opcjonalne. Zaznacz tak, jeśli możesz dostarczyć SBOM-for-AI zgodnie z minimalnymi elementami G7 (maj 2026). Dokumentuje metadane, modele, dane treningowe, infrastrukturę, właściwości bezpieczeństwa, KPI i zachowanie systemu. Standard dobrowolny.

URL dokumentu SBOM-for-AI

URL · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(D) / ENISA TIG §5.1.2

Publiczny lub udostępniony URL do Twojego dokumentu SBOM-for-AI. Może to być plik PDF, plik JSON lub strona projektu.

3. Specyficzne dla SaaS

5 pól

Region hostingu

STRING · WARUNKOWE · PODSTAWA PRAWNA: ENISA TIG §5.2

Region chmury, w którym hostowane są dane klientów. Przykład: AWS eu-central-1, Azure West Europe. Podaj region główny; regiony zapasowe lub do tworzenia kopii zapasowych można dodać po przecinku.

Szyfrowanie danych w spoczynku

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Zaznacz tak, jeśli dane klientów na dysku są szyfrowane w spoczynku za pomocą AES-256 lub równoważnego standardu. Liczy się szyfrowanie dysków zarządzane przez chmurę (AWS EBS, Azure Disk Encryption).

Szyfrowanie podczas przesyłania (TLS ≥ 1.2)

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Zaznacz tak, jeśli wszystkie punkty końcowe dostępne dla klientów wymuszają TLS 1.2 lub wyższy. Preferowany jest TLS 1.3. Zwykły HTTP musi przekierowywać na HTTPS.

MFA wymuszone dla wszystkich kont administracyjnych

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(J) / ENISA TIG §11.3

Zaznacz tak, jeśli każde wewnętrzne konto administracyjne na platformie SaaS musi używać MFA. Ten sam standard co Twoja wewnętrzna polityka administracyjna.

Docelowy czas przywrócenia (RTO) w godzinach

INTEGER · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(C) / ENISA TIG §4

Maksymalna liczba godzin, przez które Twoja usługa może być niedostępna przed przywróceniem. Realistyczna wartość SLA, a nie wartość docelowa. Typowe wartości SaaS: 4, 8 lub 24 godziny.

4. Specyficzne dla On-Premise

4 pól

Dostarczanie wykazu komponentów oprogramowania (SBOM)

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: CRA / NIS2 ART. 21(2)(D)

Zaznacz tak, jeśli dostarczasz wykaz komponentów oprogramowania (SBOM) z każdym wydaniem. CycloneDX lub SPDX to formaty standardowe. Obowiązkowe na mocy Cyber Resilience Act dla produktów wprowadzanych na rynek UE od grudnia 2027 r.

Wydania są podpisane kryptograficznie

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(E) / ENISA TIG §6.5

Zaznacz tak, jeśli każdy artefakt wydania ma podpis kryptograficzny, który klienci mogą zweryfikować. Klucze podpisujące są udokumentowane i podlegają rotacji. Liczą się zarówno podpisy Sigstore, jak i PGP.

Opublikowana polityka ujawniania podatności

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(E) / ENISA TIG §3

Zaznacz tak, jeśli masz publicznie udokumentowany sposób zgłaszania podatności bezpieczeństwa. Wystarczy plik security.txt w Twojej domenie (zgodnie z RFC 9116) lub dedykowany adres e-mail, taki jak security@example.com.

SLA poprawek dla krytycznych CVE (godziny)

INTEGER · WARUNKOWE · PODSTAWA PRAWNA: CIR 2024/2690 §5.1.4(F)

Godziny od publicznego ujawnienia CVE do wydania z poprawką dla krytycznych podatności (CVSS 9.0+). Realistyczne zobowiązanie, a nie wartość docelowa. Typowe wartości: 24, 48 lub 72 godziny.

5. Professional Services

3 pól

Zakres weryfikacji przeszłości

STRING · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(I) / CIR 2024/2690 §5.1.4(C)

Opisz, w jaki sposób weryfikujesz konsultantów do stanowisk wrażliwych. Przykład: wyciąg z rejestru karnego dla wszystkich konsultantów oraz sprawdzenie referencji w przypadku zleceń obejmujących dane niejawne.

NDA zawarte ze wszystkimi konsultantami

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(I) / ENISA TIG §11.4

Zaznacz tak, jeśli każdy konsultant podpisuje umowę o zachowaniu poufności przed przydzieleniem do pracy u klienta. Jako część umowy o pracę albo jako odrębne NDA.

Udokumentowana polityka zachowania w siedzibie klienta

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Zaznacz tak, jeśli masz pisemny kodeks postępowania dla konsultantów pracujących w siedzibie klienta: obsługa identyfikatorów, obowiązek blokowania ekranu, postępowanie w przypadku wyniesienia danych z lokalizacji.

6. Managed Services

3 pól

Wdrożone zarządzanie dostępem uprzywilejowanym (PAM)

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Zaznacz tak, jeśli używasz narzędzia do zarządzania dostępem uprzywilejowanym dla administracyjnych sesji zdalnych w systemach klientów. Przykłady: CyberArk, BeyondTrust, Teleport. Konfiguracja jump-host z rejestrowaniem logów się liczy.

Sesje administracyjne są rejestrowane

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(F) / ENISA TIG §10

Zaznacz tak, jeśli sesje administracyjne w systemach klientów są rejestrowane i przechowywane do celów weryfikacji. Typowy okres przechowywania: od 90 dni do 1 roku. Niezbędne do rekonstrukcji forensycznej po incydentach.

Dyżur 24/7

BOOLEAN · WARUNKOWE · PODSTAWA PRAWNA: NIS2 ART. 21(2)(B) / ENISA TIG §3

Zaznacz tak, jeśli prowadzisz dyżur 24/7, który reaguje na incydenty bezpieczeństwa w systemach klientów. Wsparcie wyłącznie w godzinach pracy nie spełnia tego wymogu.