18.09.2026 r.

Fundusze Europejskie

Od RODO do NIS2

Jak skutecznie zarządzać bezpieczeństwem danych w zamówieniach publicznych

Eryk Brodnicki, Open Nexus

Warszawa, 18 września 2026 r.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Eryk Brodnicki, EMBA

18.09.2026 r.

- Koordynator ds. NATO SECRET w Open Nexus Sp. z o.o.
- Audytor wiodący SZBI ISO 27001 PCA
- Audytor wiodący SZCD ISO 22301 PCA
- Inspektor Ochrony Danych
- Licencjonowany detektyw
- Prezes zarządu Centrum Audytu Bezpieczeństwa Sp. z o.o.

18.09.2026 r.


Cyberbezpieczny Samorząd
W terenie,
blisko samorządów
ROZMOWY. AUDYTY. SZKOLENIA. PRAKTYCZNE ROZWIĄZANIA.
15 na 16
WOJEWÓDZTW
odwiedzonych w ramach programu
Cyberbezpieczny Samorząd
ponad 90 000
PRZEJECHANYCH KILOMETRÓW
jedna wspólna misja – bezpieczne samorządy
Setki spotkań
URZĘDY. LUDZIE. WYZWANIA.
REALNE ROZWIĄZANIA.
Bezpieczny samorząd
to silna Polska
Samorządy
w całej Polsce
Pomorskie
Zachodniopomorskie
Warmińsko-
mazurskie
Kujawsko-
pomorskie
Podlaskie
Lubuskie
Wielkopolskie
Mazowieckie
Łódzkie
Dolnośląskie
Lubelskie
Opolskie
Śląskie
Świętokrzyskie
Małopolskie
Podkarpackie
Odwiedzone województwa
Nieodwiedzone województwo
WSPÓLNIE DLA BEZPIECZNYCH
ZAMÓWIEŃ PUBLICZNYCH

Zacznijmy od podstawowego pytania

Podpisaliśmy umowę. Dostawca dostaje dostęp administracyjny do systemu.

SKĄD WIEMY, ŻE TEN DOSTAWCA JEST BEZPIECZNY?

Nie pytamy o deklarację. Pytamy o dowody.

18.09.2026 r.

Podpisanie umowy nie kończy ryzyka

18.09.2026 r.

Jeden zakup. Trzy perspektywy.

Ryzyko powstaje na styku prawa, technologii i procesu zakupowego.

RODO

- dane osobowe
- poufność
- integralność
- dostępność

CYBERBEZPIECZEŃSTWO

- system
- usługa
- odporność
- incydenty
- ciągłość łańcuch dostaw

ZAMÓWIENIA

- wymagania
- wybór
- umowa
- nadzór
- rozliczenie dostawcy

Problem zaczyna się wtedy, kiedy te trzy światy ze sobą nie rozmawiają.

Bezpieczeństwo działa dopiero wtedy, gdy te trzy światy ze sobą współgrają.

18.09.2026 r.

RODO: „odpowiednie środki”

Art. 32 nie daje listy zakupowej. Wymaga podejścia opartego na ryzyku.

RYZYKO → **ADEKWATNE ZABEZPIECZENIA** → **ZDOLNOŚĆ DO WYKAZANIA**

POUFNOŚĆ	INTEGRALNOŚĆ	DOSTĘPNOŚĆ	ROZLICZALNOŚĆ

Inne ryzyko: zakup papieru do drukarek.

Inne ryzyko: utrzymanie systemu z danymi mieszkańców.

18.09.2026 r.

Od RODO do NIS2 / KSC

Perspektywa rozszerza się z ochrony danych na odporność całej usługi.

RODO

DANE OSOBOWE

NIS2 / KSC

RYZYKO • SYSTEM • USŁUGA
DOSTAWCA • INCYDENT • CIĄGŁOŚĆ

W Polsce nowelizacja KSC obowiązuje od kwietnia 2026 r.

18.09.2026 r.

Dostawca jest częścią Twojego ryzyka

Outsourcing usługi nie oznacza outsourcingu zarządzania ryzykiem.

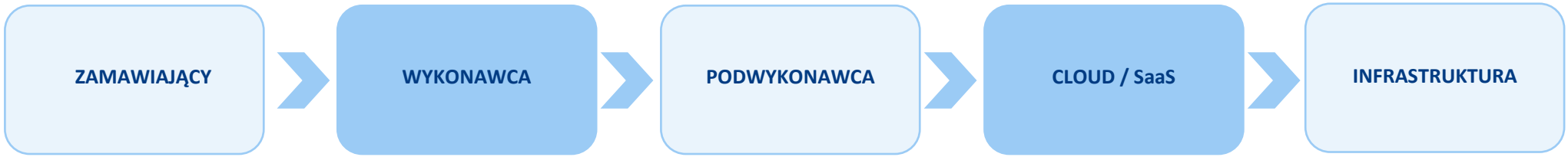
DOSTAWCA = **CZĘŚĆ TWOJEGO RYZYKA**

NIS2 wskazuje wprost bezpieczeństwo łańcucha dostaw oraz relacje z bezpośrednimi dostawcami i usługodawcami.

18.09.2026 r.

Łańcuch, którego często nie widzimy

Zamawiający zna wykonawcę. Ryzyko może sięgać znacznie dalej.



Kto faktycznie ma dostęp do danych, systemów i kopii?

Bezpieczeństwo dostawcy trzeba oceniać przez cały cykl życia usługi.

18.09.2026 r.

Najgorsze pytanie w ankiecie bezpieczeństwa

Pytanie zamknięte daje nam zamkniętą wiedzę.

„Czy zapewniają Państwo zgodność z RODO?”

☑ TAK

I czego się właśnie dowiedzieliśmy?

NICZEGO.

Pytaj: jak? Kto? Gdzie? Kiedy? Czym to wykażecie?

Zamiast deklaracji — dowody

Im większe ryzyko usługi, tym mocniejsza powinna być weryfikacja.

DEKLARACJA	DOWÓD
„stosujemy odpowiednie środki”	**raport / audyt / test**
„regularnie robimy backup”	**test odtworzeniowy**
„mamy procedurę incydentową”	**procedura + rejestry + SLA**

18.09.2026 r.

10 pytań do dostawcy

Krótka lista, która zmienia rozmowę z „czy?” na „jak?”.

1. Gdzie będą dane?
2. Kto ma dostęp?
3. Podwykonawcy?
4. MFA dla adminów?
5. Podatności?
6. Backup i retencja?
7. Test odtworzenia?
8. Zgłoszenie incydentu?
9. Jak zweryfikujemy?
10. Co po końcu umowy?

18.09.2026 r.

Incydent: 72 godziny to nie SLA dostawcy

Nie kopiuj terminu administratora do obowiązków procesora lub dostawcy.

72 h

administrator → organ nadzorczy

„w miarę możliwości, nie później niż…”

BEZ ZBĘDNEJ ZWŁOKI

podmiot przetwarzający → administrator

Umowne czasy reakcji powinny dawać zamawiającemu realny czas na analizę, ograniczenie skutków i wykonanie własnych obowiązków.

18.09.2026 r.

Backup ≠ ciągłość działania

Kopia jest wartościowa dopiero wtedy, gdy umiemy ją odtworzyć.

„Robimy backup codziennie.” → **„Czy go odtworzyliśmy?”**

RPO	RTO	IMMUTABLE	TEST
ile danych możemy utracić?	ile możemy nie działać?	czy ransomware skasuje kopię?	czy odtworzenie działa?

Dostęp administracyjny: „kto, kiedy, do czego?”

W incydencie „firma zewnętrzna miała dostęp” nie wystarcza.

VPN + LOGIN + HASŁO

wspólne konto „admin”

MFA + INDYWIDUALNE KONTO

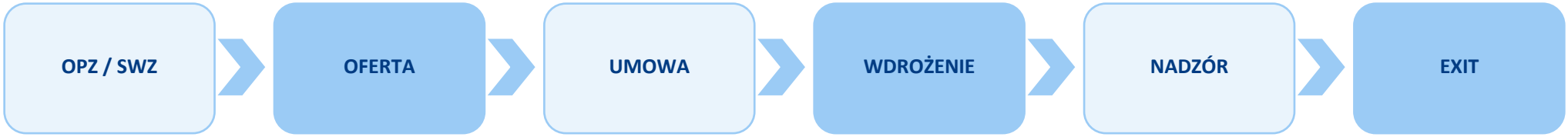
minimalne uprawnienia • czasowy dostęp
logowanie • monitoring • rozliczalność

Dostęp uprzywilejowany to jedno z miejsc, gdzie wymagania umowne muszą spotkać się z konfiguracją techniczną.

18.09.2026 r.

Bezpieczeństwo trzeba kupić

Wymaganie, które pojawia się dopiero przy podpisaniu umowy, często pojawia się za późno.



SECURITY BY PROCUREMENT

Bezpieczeństwo ma koszt — wykonawca musi znać wymagania odpowiednio wcześnie.

18.09.2026 r.

Umowa bezpieczeństwa: osiem rzeczy do dopięcia

Nie 50 stron „na wszelki wypadek”. Wymagania proporcjonalne do ryzyka.

INCYDENTY	**AUDYT**	**PODWYKONAWCY**	**BACKUP**
LOGI	**PODATNOŚCI**	**CIĄGŁOŚĆ**	**EXIT**

Najważniejsze: kto odpowiada, jaki jest czas reakcji, jaki dowód otrzymuje zamawiający.

Najbardziej niedoceniany moment? Koniec umowy.

Po kilku latach dostawca może posiadać znacznie więcej niż „nasze dane”.

EXIT

- DANE
- KONTA
- KLUCZE
- BACKUP
- LOGI
- TOKENY
- INTEGRACJE
- KONFIGURACJA

Odzyskanie danych • wyłączenie dostępów • potwierdzenie usunięcia • ciągłość usługi

Najczęstsze błędy

Problemem rzadko jest brak kolejnego dokumentu. Częściej — brak połączenia ryzyka z wymaganiem.

01 Kopiowanie wymagań z poprzedniego postępowania

02 „Zgodność z RODO” zamiast konkretów

03 Brak klasyfikacji dostawców

04 Brak weryfikacji deklaracji

05 Brak kontroli podwykonawców

06 Brak wymagań incydentowych

07 Brak planu wyjścia / migracji

18.09.2026 r.

5 pytań przed podpisaniem umowy

Slajd do zabrania ze sobą.

1

CO

powierzamy?

2

KOMU

powierzamy?

3

JAK

będzie chronione?

4

JAK

to zweryfikujemy?

5

CO

gdy coś pójdzie źle?

Jeśli nie znamy odpowiedzi — nie znamy jeszcze ryzyka dostawcy.

18.09.2026 r.

NIS2 / KSC: to dzieje się teraz

Stan na 18 września 2026 r. — trwa okres wykonywania nowych obowiązków.

3 PAŹDZIERNIKA 2026 r.

termin samorejestracji
dla podmiotów objętych tym trybem

3 KWIETNIA 2027 r.

wdrożenie obowiązków i S46
dla podmiotów w okresie przejściowym

3 KWIETNIA 2028 r.

pierwszy obowiązkowy audyt
dla wskazanych podmiotów kluczowych

Ważne: podmioty publiczne należą do grup wpisywanych do Wykazu KSC z urzędu.

18.09.2026 r.

RODO + NIS2/KSC + zamówienia

Trzy perspektywy, jeden cel: kontrolowane ryzyko dostawcy.

RODO

CHROŃ DANE OSOBOWE

NIS2 / KSC

ZARZĄDZAJ RYZYKIEM I ODPORNOŚCIĄ

ZAMÓWIENIA

PRZEŁÓŻ TO NA WYMAGANIA

WERYFIKUJ. NIE TYLKO DEKLARUJ.

Po NIS2 bezpieczeństwo dostawcy staje się bezpieczeństwem zamawiającego.

Fundusze Europejskie

Dziękuję Państwu za uwagę!