NIS2 a RODO

jeden incydent, dwa reżimy, dwie instytucje

dr Paula Skrzypecka

Jedno zdarzenie o wielu twarzach

Reżim	Nazwa zdarzenia	Akt prawny
Cyberbezpieczeństwo	incydent → incydent poważny (i krytyczny)	NIS2 - UKSC
Ochrona danych	naruszenie ochrony danych osobowych	RODO
Sektor finansowy	poważny incydent związany z ICT	DORA (przepis szczególny)

Nie wszystkie te akty prawne działają tak samo

Ranga i tryb

RODO = rozporządzenie - działa wprost, jednolicie w UE

NIS2 = dyrektywa - wiąże nas nie ona, lecz polska UKSC

DORA = rozporządzenie - dla finansów lex specialis wobec NIS2 (pierwszeństwo)

Polska UKSC dodała ponad dyrektywę:

- rejestr podmiotów z oświadczeniami pod rygorem karnym
- mechanizm dostawcy wysokiego ryzyka · szkolenia kierownictwa · weryfikacja niekaralności (KRK)

Kary się kumulują

Triada CIA - most między światami

Triada CIA (ISO 27001, NIS2)	Art. 4 pkt 12 RODO
Poufność (C)	nieuprawnione ujawnienie lub dostęp
Integralność (I)	modyfikacja
Dostępność (A)	zniszczenie, utrata

Incydent cyber staje się naruszeniem RODO w momencie, w którym narusza C, I lub A danych osobowych.

„Nie mamy dowodu” vs. „nie możemy wykluczyć”

Prawo karne

Domniemanie niewinności

RODO, NIS2 - odwrotnie

Czy potrafimy wykluczyć nieuprawniony dostęp?

„Mamy 72 godziny” w praktyce

	UKSC / NIS2	RODO
Start zegara	od wykrycia incydentu	od stwierdzenia naruszenia
Adresat	CSIRT (przez system S46)	Prezes UODO
Druga komunikacja	użytkownicy usługi	osoby, których dane dotyczą (art. 34)

Dwa pistolety startowe: zegar UKSC rusza zwykle pierwszy (SOC wykrywa, zanim prawnik potwierdzi kwalifikację RODO). To jest OK - pod warunkiem, że obie narracje będą potem spójne.

Konsekwencja: wczesne ostrzeżenie do CSIRT zwykle wychodzi, zanim w ogóle podejmiecie decyzję o UODO..

Kaskada UKSC - do CSIRT

24 h

Wczesne ostrzeżenie

niezwłocznie, ≤ 24 h od wykrycia

72 h

Zgłoszenie incydentu poważnego

≤ 72 h od wykrycia

1 mc

Sprawozdanie końcowe

≤ miesiąc od zgłoszenia

Jeśli obsługa trwa - sprawozdanie z postępu w międzyczasie, końcowe miesiąc po domknięciu.

Adresat: docelowo CSIRT sektorowy; w trybie przejściowym (do ogłoszenia jego zdolności) - krajowy: **CSIRT NASK/CSIRT GOV/CSIRT MON**. Kanał: system S46. Wybór CSIRT wynika z sektora, nie z decyzji podmiotu.

Zdolność do zgłoszenia w 24 h musi działać od dnia obowiązywania - nawet jeśli CSIRT sektorowy jeszcze nie ruszył.

Kaskada RODO - art. 33 i art. 34

Art. 33 - UODO

bez zbędnej zwłoki, w miarę możliwości **≤ 72 h od stwierdzenia** - chyba że mało prawdopodobne, by skutkowało ryzykiem dla praw i wolności.

Art. 34 - ludzie

- bez zbędnej zwłoki, gdy ryzyko wysokie
- art. 33 ust. 4: zgłoszenie etapowe - informacje sukcesywnie
- art. 33 ust. 5: każde naruszenie do rejestru wewnętrznego, także niezgłoszone

Kiedy „stwierdzamy”? Gdy mamy rozsądny stopień pewności że doszło do naruszenia danych - nie przy pierwszym alercie, ale też nie po trzech tygodniach.

Metoda trzech koszyków - jak pisać, żeby nie zaszkodzić?

1 Co wiemy?

fakty

szyfrowanie, liczba serwerów, treść noty, czas wykrycia

2 Czego nie wiemy?

jawnie, uczciwie

„nie ustaliliśmy dotąd zakresu eksfiltracji”

3 Co wykluczyliśmy?

tylko z dowodem

„na podstawie logów proxy wykluczyliśmy transfer z segmentu B”

Trzy zakazy językowe:
żadnych absolutów („wszystkie”, „żadne”, „w pełni”, „całkowicie”) · zawsze kotwica czasowa („na obecnym etapie”) · nie myl „nie wiemy” z „wykluczyliśmy”

„Nie wykryliśmy oznak eksfiltracji” - bezpieczne. „Eksfiltracja nie nastąpiła” - ryzykowne.

Fun fact: sposób obsługi tych 72 h obniża karę

Art. 83 RODO: 11 czynników

na które macie wpływ W TRAKCIE:

- terminowość i inicjatywa zgłoszenia
- współpraca z organem
- wdrożone środki
- umyślność vs. niedbalstwo

Za co podwyższano kary?

brak zgłoszenia, potem wyjaśnienia lakoniczne i niespójne · pisma niepodpisane przez osoby uprawnione · odpowiedziała inna spółka niż wezwana.

Niespójność i niechlujstwo wobec regulatora = samodzielny czynnik obciążający.

Dwa audytoria każdego zdania: regulator + przyszły powód (+ rynek).

Rozwiązanie wzorcowe - cztery decyzje

1	**CSIRT - TAK, pierwszy ruch**	incydent poważny (przerwana ciągłość usługi kluczowej). Wczesne ostrzeżenie ≤24 h (realnie sobota rano); brak zdolności sektorowego → krajowy, przez S46.
2	**UODO - TAK**	min. naruszenie dostępności; wobec noty grożącej publikacją założyć też poufność (nie można wykluczyć eksfiltracji). Dane medyczne (art. 9) → ryzyko wysokie.
3	**Ludzie - TAK, z timingiem**	najpierw zgłoszenie do UODO + ustalenie zakresu, potem zawiadomienie osób. Równolegle info dla użytkowników usługi o niedostępności.
4	**Pierwsze zgłoszenie**	fakty + „nie można wykluczyć” eksfiltracji + środki + szacunek oznaczony jako wstępny. Do aktualizacji: potwierdzenie eksfiltracji, zakres, root cause, IoC/TTP.

Sześć pytań pierwszej godziny - minimalny playbook decyzyjny

1 **Co dokładnie obserwujemy?**

fakty, nie hipotezy. Który atrybut CIA?

2 **Czy dotknięte są dane osobowe?**

jeśli nie wiemy - zakładamy, że tak

3 **Czy ucierpiała usługa/systemy?**

to uruchamia reżim UKSC

4 **Który zegar ruszył i kiedy?**

zanotuj moment wykrycia - będzie kwestionowany

5 **Czy możemy cokolwiek wykluczyć?**

bez logów zakładamy najgorszy scenariusz

6 **Kto musi być w pokoju w ciągu godziny?**

koordynator, IT, IOD, prawnik, ktoś z zarządu…

Matryca playbooka: zdarzenie → próg → adresat → termin → właściciel

Zdarzenie	Próg	Adresat	Termin	Właściciel
Incydent poważny	wpływ na usługę/systemy	CSIRT (S46)	24h/72h/1mc	Koordynator+SOC
Naruszenie danych	ryzyko dla praw i wolności	UODO	72h od stwierdzenia	IOD → ADO
Wysokie ryzyko	wysokie ryzyko	osoby fizyczne	bez zbędnej zwłoki	ADO + prawnik
Wpływ na usługę	poważny incydent	użytkownicy usługi	niezwłocznie	biznes + PR
Każde naruszenie	zawsze	rejestr wewn. (33 ust. 5)	na bieżąco	IOD