

Dazr Compliance · Karta produktu · Zarządzanie incydentami

Każdy *termin* incydentu, odliczany.

Zarejestruj incydent, a zegary ruszają: 72 godziny na zgłoszenie z art. 33 RODO oraz 24 godziny, 72 godziny i miesiąc dla NIS2. Narzędzie oparte na rozporządzeniu wykonawczym (UE) 2024/2690 mówi, czy incydent jest istotny. Rejestr incydentów jest w każdym planie, także w Free.

Edytuj incydent



Zapisano 2 paź 2026, autor: sanne.devries@brightwater.example

Naruszenie ochrony danych osobowych: licznik 72 godzin z RODO

● **Zgłoszenie do organu za 17 godz.**

Zgłoś naruszenie organowi nadzorczemu w ciągu 72 godzin od wykrycia (art. 33 RODO): do 3 paź 2026, 10:49. Do czasu wlicza się weekendy.

Tytuł

Wypis ze szpitala wysłany e-mailem do niewłaściwej przycz

Waga

● Niska ● Średnia ● **Wysoka** ● Krytyczna

Status

W badaniu Opanowany Rozwiązany Zamknięty

Najważniejsze funkcje

- ✓ **Zegar RODO:** 72 godziny od powzięcia wiadomości na zgłoszenie do organu nadzorczego (art. 33).
- ✓ **Kamienie milowe NIS2:** wczesne ostrzeżenie po 24 godzinach, zgłoszenie po 72 godzinach, raport końcowy w ciągu miesiąca (art. 23).
- ✓ **Narzędzie do oceny istotnych incydentów** oparte na rozporządzeniu wykonawczym (UE) 2024/2690.
- ✓ **Pola zgłoszenia**, o które pyta organ, oś czasu, przyczyna źródłowa i wyciągnięte wnioski.
- ✓ **Publiczny portal zgłaszania naruszeń** w planie Enterprise: zgłoszenia bez konta, zatwierdzane do rejestru.

Zegary RODO i NIS2

Każdy incydent pokazuje odliczanie od chwili, gdy się o nim dowiedziałeś. Naruszenie ochrony danych osobowych uruchamia zegar z art. 33 RODO: 72 godziny na zgłoszenie organowi nadzorcemu, wliczając weekendy. Istotny incydent NIS2 uruchamia kamienie milowe z art. 23: wczesne ostrzeżenie w ciągu 24 godzin, zgłoszenie incydentu w ciągu 72 godzin i raport końcowy w ciągu miesiąca. Zapisz, kiedy każde z nich wysłano, a zegar przeskakuje do następnego.

Dazr zapisuje pola i znaczniki czasu; samo zgłoszenie nadal składa się w portalu Twojego organu. Wypróbuj bezpłatny kalkulator terminu zgłoszenia naruszenia.

Czy to istotny incydent według NIS2?

Narzędzie do oceny istotnych incydentów przechodzi przez kryteria rozporządzenia wykonawczego (UE) 2024/2690 dla podmiotów infrastruktury cyfrowej i dostawców cyfrowych, które obejmuje, na podstawie typów podmiotów i obrotu z Twojego profilu zgodności. Wynik, spełnione kryteria i czas sprawdzenia są zapisywane przy incydencie, a wynik „istotny” włącza kamienie milowe NIS2. Na tej stronie jest też bezpłatne narzędzie do oceny istotnych incydentów NIS2.

Co zawiera rekord incydentu

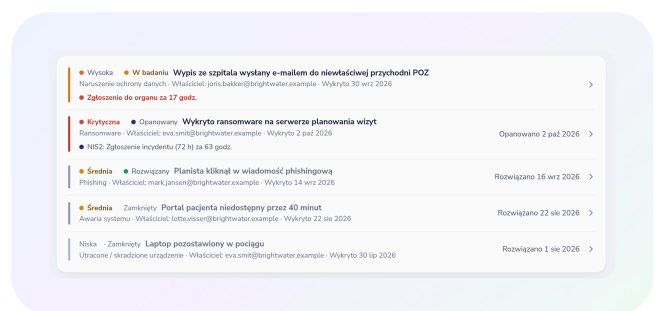
- Typ (dwanaście, od naruszenia danych i ransomware po incydenty u dostawców i fizyczne), istotność i status od badania do zamknięcia.
- Kiedy wystąpił, został wykryty, opanowany, kiedy usunięto przyczyny i rozwiązano go oraz przez kogo.
- Pola z art. 33: rodzaje danych, których dotyczy, i przybliżona liczba osób, których dane dotyczą, prawdopodobne skutki, podjęte środki, kontakt do IOD, organ, data zgłoszenia i numer sprawy oraz informacja, czy osoby, których dane dotyczą, zostały powiadomione.
- Oś czasu zdarzeń, przyczyna źródłowa, ograniczanie skutków i wyciągnięte wnioski, z linkiem do zabezpieczenia korygującego lub zadania.
- Wykres incydentów według istotności w rejestrze oraz rejestr w eksportach do Excela i CSV.

Publiczny portal zgłaszania naruszeń

W planie Enterprise administrator włącza stronę zgłoszeń i udostępnia jej link. Każdy może zgłosić podejrzenie naruszenia bez konta: proste pytania i przestanie zrzutu ekranu. Lista dozwolonych domen e-mail, kontrola proof-of-work oraz limity godzinowe i dzienne trzymają spam z daleka. Zgłoszenia trafiają do kolejki, z której Twoja osoba odpowiedzialna za bezpieczeństwo zatwierdza je do rejestru incydentów albo odrzuca.

Na telefonie, gdy to ważne

Portal działa na telefonie, po angielsku, niderlandzku, włosku, niemiecku, francusku, hiszpańsku i polsku, na chwile, gdy incydent nie poczeka na laptopa. Członkom przypisuje się incydenty, audytorzy dodają notatki, a webhooks w planie Enterprise wysyłają zdarzenia incydentów do Twojego systemu ticketów lub czatu.



Platforma

- | | | |
|---|--|--|
| ✓ Hosting w UE, tworzone przez Dazr we Włoszech | ✓ Dane szyfrowane w spoczynku (AES-256-GCM) | ✓ Logowanie przez Google, Microsoft lub kod e-mail |
| ✓ Role: właściciel, administrator, członek, audytor | ✓ Przeszukiwalny dziennik aktywności z eksportem | ✓ Angielski, niderlandzki, włoski, niemiecki, francuski, hiszpański i polski |

Plany: Free 0 € · Basic 29 € · Pro 99 € · Enterprise 499 € miesięcznie, netto · Custom na zapytanie

Więcej na compliance.dazr.eu/pl/funkcje/zarzadzanie-incydentami · sales@dazr.eu · Dazr, Włochy · NIP IT 02801250065

Umów demo
compliance.dazr.eu