COMPLIANCE

KALENDARZ

2026

AI ACT, ESG, NIS2, ISO27001, CYBERSECURITY

Quantifier.ai

Droga Użytkowniczko,
Drogi Użytkowniku Kalendarza

W świecie, w którym przepisy zmieniają się szybciej niż cykle technologiczne, a odpowiedzialność zarządcza staje się jednym z kluczowych elementów przewagi konkurencyjnej, skuteczne prowadzenie organizacji wymaga nie tylko narzędzi, lecz także świadomości, rytmu i konsekwencji.

Ten kalendarz powstał jako praktyczne wsparcie dla firm, które traktują compliance, bezpieczeństwo informacji, ESG i odpowiedzialny rozwój nie jako obowiązek, lecz jako fundament nowoczesnego zarządzania.

Każdy miesiąc prowadzi przez najważniejsze obszary regulacyjne i operacyjne od ochrony danych, przez cyberbezpieczeństwo, ryzyko i ciągłość działania, po łańcuch dostaw, etykę, ESG, sztuczną inteligencję, a na KYC/AML kończąc. Tematy te nie są przypadkowe. Odzwierciedlają realne wyzwania, z którymi mierzą się organizacje w Europie i na świecie, oraz odpowiadają harmonogramowi kluczowych międzynarodowych wydarzeń i dni tematycznych.

Mamy nadzieję, że ten kalendarz pomoże w planowaniu, porządkowaniu priorytetów i budowaniu przewagi opartej na odpowiedzialnym, dojrzałym i świadomym podejściu do zarządzania. To narzędzie, które ma inspirować, ułatwiać i wspierać — przez cały rok.

Życzymy dobrego, mądrego i bezpiecznego roku operacyjnego.

Zespół Enwirly Quantifier

Autonomiczny compliance officer w erze AI

Quantifier.ai na nowo definiuje sposób, w jaki firmy podchodzą do compliance - dzięki działającej nieprzerwanie, autonomicznej platformie AI, która monitoruje, egzekwuje i prowadzi działania regulacyjne w całej organizacji. Quantifier tworzy nową kategorię: inteligentny, proaktywny i w pełni autonomiczny compliance.

Rozszerzamy się obecnie do pełnej platformy, która automatyzuje wszystko - od analityki regulacyjnej i przygotowania do audytu po zarządzanie projektami i ograniczanie ryzyka. Tam, gdzie tradycyjne narzędzia SaaS opierają się na pracy ludzi i kosztownych konsultantach, Quantifier działa w sposób ciągły i autonomiczny, obniżając koszty, oszczędzając czas i zapewniając spokój w skali całej organizacji.

Pozyskujemy kapitał, aby rozwinąć Quantifier do roli dominującej warstwy infrastruktury AI dla globalnego compliance. Skala tej szansy jest ogromna.

Envirly to marka Quantifier odpowiedzialna za obszar ESG i zrównoważonego rozwoju. Wspieramy organizacje w spełnianiu wymogów środowiskowych i klimatycznych — poprzez:

- raportowanie ESG zgodne z CSRD i ESRS,
- obliczanie śladu węglowego w zakresach 1, 2 i 3 (GHG Protocol),
- środowiskowe oceny cyklu życia produktów (LCA),
- działania doradcze i wdrożeniowe w obszarze redukcji emisji.

Quantifier.ai

envirly

2026

Styczeń

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Luty

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Marzec

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Kwiecień

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Maj

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Czerwiec

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Lipiec

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Sierpień

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Wrzesień

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	29
20	21	22	23	24	25	26
27	28	29	30			

Październik

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Listopad

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Grudzień

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

STYCZEŃ

Miesiąc ochrony danych osobowych

Twoje dane to Twój skarb – jak RODO zmieniło zasady gry w ochronie prywatności.

Miesiąc bezpieczeństwa danych

W styczniu skupiamy się na ochronie danych osobowych. RODO (GDPR) nałożyło na organizacje surowe obowiązki w zakresie przetwarzania danych – od uzyskiwania świadomych zgód po raportowanie naruszeń w 72 godziny. Dziś prywatność to nie tylko wymóg prawny, ale element reputacji firmy. 28 stycznia obchodzimy Dzień Ochrony Danych Osobowych, przypominający, że świadome zarządzanie informacjami to podstawa zaufania klientów. Mimo iż minęło już kilka lat od wejścia RODO, presja regulacyjna nie maleje – organy nadzorcze nakładają coraz wyższe kary za uchybienia. Łącznie w całej Europie wydano już ponad 2,6 tys. decyzji o karach, na sumę ok. 5,65 mld euro(największa – 1,2 mld euro dla Meta w 2023).

W Polsce również egzekwowanie przepisów przyspiesza: **do 2025 r. UODO nałożył 88 kar na łączną kwotę ponad 12 mln euro.** Co więcej, Polacy zgłaszają bardzo dużo incydentów – w 2024 r. zgłoszono w Polsce 14,2 tys. naruszeń danych (trzecie miejsce w Europie). Te statystyki pokazują, że ochrona danych to realne wyzwanie – dlatego w styczniu warto zrobić przegląd zgodności z RODO i zadbać o utrwalenie kultury prywatności w firmie.

Kluczowe statystyki

5,65 mld €

suma kar nałożonych w Europie za naruszenia RODO (2018–2025)*

12 mln €

Łączna kwota kar RODO na polskie firmy od 2018r. (88 decyzji Prezesa UODO)**

Quantifier.ai

* https://cms.law/en/pol/news-information/record-broken-gdpr-fines-exceed-eur-5-billion-for-the-first-time
** https://resilia.pl/blog/rejestr-kar-rodo-polskie-firmy-od-momentu-wprowadzenia/

Case study: Automatyzacja zgodności z RODO.

Średniej wielkości firma zdecydowała się wdrożyć platformę Quantifier, aby uporządkować procesy związane z ochroną danych osobowych i zmniejszyć ryzyko naruszeń. Dzięki rozwiązaniu opartemu na automatyzacji i sztucznej inteligencji organizacja zyskała pełną kontrolę nad kluczowymi obowiązkami wynikającymi z RODO.

Platforma samodzielnie prowadzi Rejestr Czynności Przetwarzania, monitoruje terminy retencji oraz obsługuje wnioski osób, których dane dotyczą — od żądania dostępu po usunięcie — zamykając je w przejrzystym, ustandaryzowanym workflow. W sytuacji potencjalnego incydentu, np. wycieku danych, system automatycznie uruchamia procedurę reagowania: wskazuje konieczne działania, wspiera analizę ryzyka i pomaga przygotować kompletne zgłoszenie do UODO w przewidzianym przepisami terminie.

Efekty:
Firma skróciła średni czas reakcji na incydent o 50%, ograniczyła liczbę błędów proceduralnych i zyskała realną ochronę przed kosztownymi sankcjami.

Czy wiesz że....

RODO przewiduje drakońskie **kary finansowe – nawet do 20 mln euro** lub 4% globalnego obrotu przedsiębiorstwa za najpoważniejsze naruszenia. Dotychczas w Polsce najwyższa pojedyncza kara wyniosła ok. 4 mln zł, ale trend rosnący jest wyraźny. Co ciekawe, Polska znajduje się w czołówce Europy pod względem liczby zgłaszanych incydentów – ponad 14 tys. rocznie – co może świadczyć zarówno o dużej skali problemu, jak i rosnącej świadomości firm w zakresie obowiązku raportowania naruszeń. Z kolei od wejścia RODO w życie na polskie firmy nałożono łącznie 88 kar pieniężnych na sumę przekraczającą 12 mln euro. To dowód, że nie warto ryzykować – lepiej zainwestować w compliance niż płacić kary i tracić reputację.

Quantifier.ai

Lista kontrolna RODO – co warto sprawdzić w styczniu:

1. Czy posiadamy aktualny rejestr czynności przetwarzania danych osobowych?
2. Czy posiadamy aktualny rejestr czynności przetwarzania danych osobowych?
3. Czy wszyscy pracownicy przeszli szkolenie RODO (zwłaszcza nowo zatrudnieni)?
4. Czy procedury obsługi żądań podmiotów danych (dostęp, sprostowanie, usunięcie itp.) działają sprawnie i w terminach?
5. Czy mamy wdrożony plan reagowania na incydent bezpieczeństwa danych i czy testowaliśmy go?
6. Czy nasza polityka prywatności oraz klauzule informacyjne są zaktualizowane (np. uwzględniają nowe usługi, cookies etc.)?
7. Czy dokonaliśmy oceny ryzyka dla nowych procesów przetwarzania danych?
8. Czy wszystkie powierzenia danych (umowy z dostawcami) posiadają wymagane klauzule powierzenia?

Wyzwanie na styczeń

Przeprowadź mini-audyt RODO w swoim dziale. Sprawdź, jakie dane osobowe przechowujecie i czy na pewno macie do tego podstawę prawną. Usuń lub zanonimizuj informacje, których już nie potrzebujesz. Zachęć zespół, by 28 stycznia – w Dzień Ochrony Danych – każdy wykonał jedno działanie pro-prywatność (np. wyczyścił skrzynkę ze starych maili z danymi, poprawił hasła, włączył dwuskładnikowe uwierzytelnienie). To małe kroki, które wzmacniają kulturę ochrony danych.

Psychotest:
Którą normą ISO jesteś?

Zaznacz odpowiedzi i poznaj swój... certyfikowany charakter.

1. Jak reagujesz, gdy coś idzie niezgodnie z planem?
A. Spokojnie tworzę procedurę naprawczą i działam.
B. Zbieram dane, analizuję, robię wykres i dopiero wtedy działam.
C. Dzwonię do wszystkich i upewniam się, czy wszyscy czują się dobrze.
D. Upewniam się, że nic nie spłonie i że wszyscy są bezpieczni.

2. Co jest Twoją supermocą?
A. Organizacja i porządek w chaosie.
B. Liczby, fakty i twarde dowody.
C. Empatia i relacje.
D. Gaszenie pożarów, często dosłownie 😉

3. Gdy znajomi proponują spontaniczny wyjazd...
A. Pytam o ryzyka, dokumenty i harmonogram.
B. Liczę budżet, opcje transportu i ROI tej wycieczki.
C. Zastanawiam się, jak wpłynie to na nasz well-being.
D. Sprawdzam prognozę pogody, apteczkę i gaśnice.

4. Co wkurza Cię najbardziej?
A. Brak procedur.
B. „Słyszałem, że tak będzie" zamiast danych.
C. Brak odpowiedzialności za drugiego człowieka.
D. Chaos, który grozi katastrofą.

5. Jakim typem jesteś?
A. Poukładanym i procesowym.
B. Analitycznym i konkretnym.
C. Wspierającym i komunikacyjnym.
D. Odpornym, szybkim i gotowym na kryzys.

Wyniki
Najwięcej A: Jesteś ISO 27001 – Mistrz Porządku i Bezpieczeństwa Informacji. Kochasz procedury, kochasz kontrolę dostępu, kochasz ryzyka w tabelkach. Twoje hasło do Wi-Fi ma 38 znaków, w tym emoji i znak integralności. Chaos boi się wejść tam, gdzie Ty pracujesz.

Najwięcej B: Jesteś ISO 9001 – Szef Jakości. Jakość to dla Ciebie styl życia, a każdy proces da się zoptymalizować. W restauracji oceniasz „ciągłe doskonalenie" po samej karcie dań. Na wakacjach robisz SWOT analizy atrakcji turystycznych.

Najwięcej C: Jesteś ISO 14001 – Zielona Dusza Myślisz o wpływie na środowisko — i ludzi. Znasz losy każdego kubka papierowego w biurze. Twoje rośliny w domu mają lepszą opiekę niż większość korporacji.

Najwięcej D: Jesteś ISO 45001 – Strażnik Bezpieczeństwa. Zawsze w trybie „anti-accident mode". Z Tobą nikt nie skręci kostki, nie zachłyśnie się kawą i nie potknie o kabel. Twoje życie to ciągły emergency drill.

28 STYCZNIA

EUROPEJSKI DZIEŃ OCHRONY DANYCH OSOBOWYCH

Ustanowione na pamiątkę Konwencji 108 Rady Europy, ma przypominać obywatelom i organizacjom o znaczeniu prywatności.

Święto sprzyja budowaniu pozytywnej narracji – pokażcie, że dbanie o dane to część Waszej misji, nie tylko obowiązek prawny.

Pogromcy mitów. Obalamy mity o RODO:

- **Mit**: „RODO dotyczy tylko danych cyfrowych, a nie papierowych dokumentów."
- **Fakt**: RODO chroni dane osobowe bez względu na formę – zarówno elektroniczną, jak i tradycyjną na papierze. Segregatory z danymi klientów też muszą być zabezpieczone.

- **Mit**: „Małe firmy nie muszą przejmować się RODO."
- **Fakt**: RODO co do zasady obejmuje wszystkie podmioty przetwarzające dane osobowe w związku z działalnością gospodarczą. Są pewne wyjątki (np. działalność czysto osobista), ale wielkość firmy nie zwalnia z odpowiedzialności. Małe firmy również muszą mieć podstawy prawne przetwarzania, realizować prawa osób i dbać o bezpieczeństwo danych – choć skala działań jest proporcjonalna do ryzyka.

Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

RODO obowiązuje nie tylko firmy z UE, ale także podmioty spoza UE, jeśli oferują towary/usługi osobom w UE lub monitorują ich zachowanie.

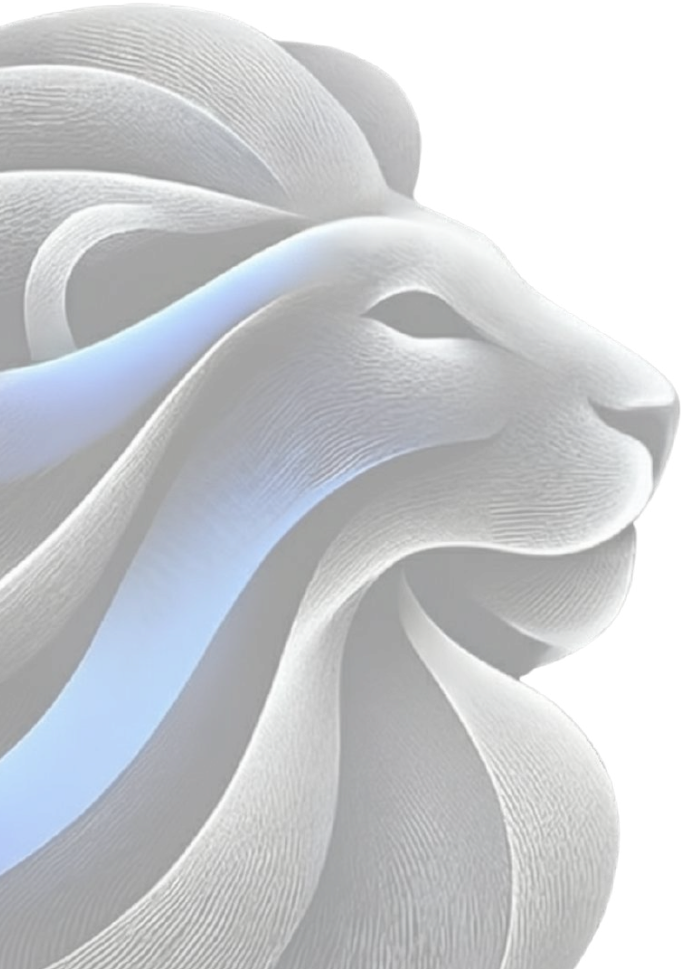
PRAWDA ☐ **FAŁSZ** ☐

Maksymalna kara administracyjna z RODO może wynieść do 4% globalnego rocznego obrotu firmy.

PRAWDA ☐ **FAŁSZ** ☐

RODO wymaga, aby każda operacja przetwarzania danych osobowych opierała się na zgodzie osoby.

PRAWDA ☐ **FAŁSZ** ☐



1 odpowiedź - prawda. 2 odpowiedź - prawda.
3 odpowiedź - fałsz

Quantifier.ai

LUTY

Miesiąc praw pracownika

Kultura zaufania i sprawiedliwości w organizacji – sygnaliści i prawa człowieka na straży etyki biznesu.

Miesiąc praw pracownika

W lutym pochylamy się nad prawami pracowników oraz szerszym tematem poszanowania praw człowieka w biznesie. To nie przypadek – 20 lutego przypada Światowy Dzień Sprawiedliwości Społecznej, podkreślający znaczenie godnych warunków pracy, równości i solidarności.

W świecie compliance kluczowe miejsce zajmuje obecnie whistleblowing, czyli systemy zgłaszania nieprawidłowości. Unijna dyrektywa o ochronie sygnalistów (2019/1937) w końcu doczekała się wdrożenia w Polsce – po wielu opóźnieniach nasza ustawa weszła w życie dopiero 25 września 2024 (Polska była ostatnim krajem UE, który ją implementował).

Nowe przepisy wymagają od firm m.in. ustanowienia wewnętrznych kanałów zgłaszania oraz ochrony przed represjami dla osób zgłaszających nadużycia. Równolegle, na horyzoncie mamy przełomową regulację UE – Corporate Sustainability Due Diligence Directive (CSDDD), która weszła w życie w lipcu 2024 i do lipca 2026 musi być zaimplementowana w krajach członkowskich.

CSDDD nałoży obowiązki należytej staranności w zakresie praw człowieka i środowiska, zmuszając duże przedsiębiorstwa do monitorowania swoich łańcuchów dostaw pod kątem np. pracy przymusowej, praw pracowniczych czy degradacji środowiska. Coraz mocniej akcentowane są także standardy międzynarodowe – Wytyczne OECD dla przedsiębiorstw wielonarodowych czy Wytyczne ONZ dot. biznesu i praw człowieka – które, choć miękkie, wyznaczają pewien wzorzec odpowiedzialnego postępowania. Krótko mówiąc: rośnie presja, by biznes działał fair play wobec pracowników, kontrahentów i społeczności.

Kluczowa statystyka

43%

odsetek nadużyć (oszustw, korupcji) wykrywanych dzięki sygnalistom (najskuteczniejszy mechanizm kontroli!).*

Quantifier.ai

* https://www.anchin.com/wp-content/uploads/2024/08/2024-ACFE-Occupational-Fraud-Report.pdf

Case study: System dla sygnalistów w praktyce**.**

Firma usługowa wdrożyła platformę Quantifer, aby wzmocnić kulturę transparentności. Pracownicy i kontrahenci zyskali bezpieczny, anonimowy kanał online do zgłaszania mobbingu, korupcji, naruszeń BHP czy fałszowania dokumentów.
System automatycznie kieruje zgłoszenia do właściwych zespołów, zapewnia poufność, umożliwia dwustronny kontakt z anonimizowanym sygnalistą i pilnuje ustawowych terminów (7 dni na potwierdzenie zgłoszenia, 3 miesiące na informację zwrotną).

Efekty po 6 miesiącach:

- wzrost liczby zgłoszeń , głównie drobnych spraw, rozwiązanych zanim przerodziły się w kryzys,
- brak wycieków informacji na zewnątrz,
- wyraźny wzrost zaufania do kierownictwa w badaniach pracowniczych,
- lepsze ukierunkowanie szkoleń etycznych dzięki analizie danych z platformy.

Wniosek:
Nowoczesne platformy realnie wzmacniają kulturę „mówienia wprost", zmniejszają ryzyko kryzysów i budują bezpieczne środowisko pracy.

Czy wiesz że....

Whistleblowing jest w praktyce najskuteczniejszym mechanizmem wykrywania nadużyć – globalne badania ACFE pokazują, że zgłoszenia wykrywają trzykrotnie więcej przypadków oszustw niż audyt wewnętrzny czy inne klasyczne kontrole.

Quantifier.ai

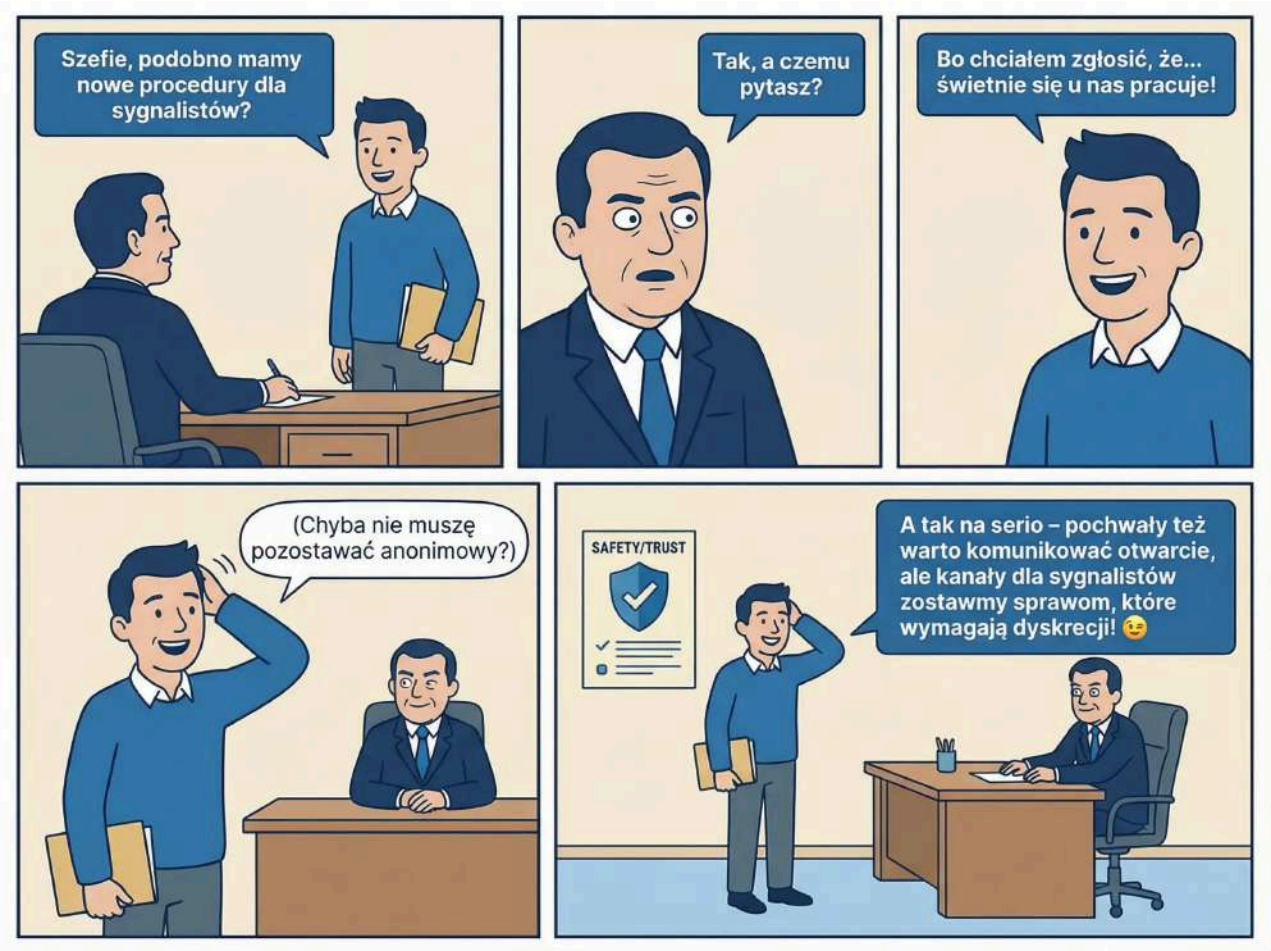
Lista kontrolna - prawa pracownika i etyka

1. Czy posiadamy formalną, zakomunikowaną politykę zgłaszania nieprawidłowości (whistleblowing) i czy każdy wie, jak z niej skorzystać?
2. Czy uruchomiliśmy anonimowy kanał dla sygnalistów (np. skrzynka, infolinia, narzędzie online) i czy jest on odpowiednio zabezpieczony pod kątem poufności?
3. Czy wyznaczyliśmy niezależną osobę lub zespół ds. obsługi zgłoszeń, który odbiera, bada i reaguje na zgłoszenia (może to być compliance officer, dział prawny lub zewnętrzny podmiot)?
4. Czy istnieją procedury zapobiegania odwetowi wobec sygnalistów oraz mechanizmy wsparcia dla nich (np. gwarancja, że zgłoszenie w dobrej wierze nie skończy się zwolnieniem ani szykanami)?
5. Czy nasz Kodeks Etyki i regulaminy wewnętrzne jasno określają prawa pracowników (np. prawo do godnego traktowania, równych szans, bezpieczeństwa) oraz obowiązki kadry kierowniczej w tym zakresie?
6. Czy przeprowadzamy szkolenia z etyki i praw człowieka dla pracowników i managerów – np. jak rozpoznawać i zgłaszać dyskryminację, mobbing, konflikty interesów?
7. Czy mamy procedury due diligence dotyczące praw człowieka w łańcuchu dostaw (np. czy sprawdzamy, czy nasi dostawcy nie łamią praw pracowniczych, czy wymagamy od nich pewnych standardów)? Już teraz warto to robić w ramach przygotowań do CSDDD.
8. Czy monitorujemy wskaźniki HR mogące wskazywać na problemy (rotacja, absencje, skargi) i czy zarząd otrzymuje regularnie raporty o stanie „kultury organizacyjnej”?

Wyzwanie na luty

Przygotuj anonimową ankietę dla pracowników dotyczącą kultury etycznej. Zapytaj, czy wiedzą jak zgłosić problem, czy czują się bezpiecznie to robiąc, i czy ufają, że firma zareaguje. Podsumuj wyniki i przedstaw plan poprawy słabych punktów.

Dodatkowo, z okazji Dnia Sprawiedliwości Społecznej (20.02) zorganizuj krótką sesję (np. webinar lub meeting) o prawach człowieka w biznesie – omów przykłady naruszeń w świecie (np. praca dzieci, dyskryminacja) i pokaż, co Wasza firma robi, by ich nie wspierać. Na koniec zaproponuj wszystkim „challenge fair play"– przez resztę miesiąca każdy zgłasza przynajmniej jeden pomysł, jak uczynić miejsce pracy bardziej przyjaznym i sprawiedliwym.



20 LUTY

ŚWIATOWY DZIEŃ SPRAWIEDLIWOŚCI SPOŁECZNEJ

Proklamowany przez ONZ, ma promować wysiłki na rzecz eliminacji ubóstwa, wykluczenia, dyskryminacji w świecie pracy. Dla firm to dobra okazja, by przypomnieć o przestrzeganiu praw pracowniczych i standardów pracy.

W okolicach tego dnia można np. opublikować wewnętrznie historię (case) pracownika, który zgłosił problem i doczekał się rozwiązania – jako inspirujący przykład.

Pogromcy mitów. Whistleblowing i praw pracownika:

- **Mit**: „Sygnalista to zawsze ‘kapuś’ działający na szkodę firmy.”
- **Fakt**: Sygnalista to osoba działająca w dobrej wierze dla dobra organizacji – ujawnia problem, zanim urośnie on do rangi poważnego kryzysu czy skandalu. Dzięki sygnalistom firma może naprawić naruszenie wewnętrznie, unikając kar i utraty wizerunku. Najczęściej motywacją sygnalistów jest poczucie sprawiedliwości, nie zemsta.
- **Mit**: „Tylko duże korporacje muszą przejmować się prawami człowieka w łańcuchu dostaw.”
- **Fakt**: Już teraz coraz więcej średnich firm spotyka się z wymaganiami od partnerów biznesowych dotyczącymi standardów etycznych. Wkrótce (CSDDD) obowiązki formalne obejmą największe firmy, ale pośrednio dotkną także mniejszych – bo duże podmioty będą wymagać od swoich dostawców poszanowania praw człowieka i środowiska. Etyka staje się warunkiem uczestnictwa w globalnym rynku, niezależnie od wielkości firmy.

Dwie prawdy i jeden fałsz.

Zaznacz prawidłową odpowiedź:

Polskie firmy zatrudniające 50 lub więcej pracowników muszą mieć wewnętrzną procedurę zgłaszania nieprawidłowości i kanał dla sygnalistów.

PRAWDA ☐ FAŁSZ ☐

Zgłoszenia mogą dotyczyć nie tylko naruszeń prawa krajowego czy unijnego, ale i np. korupcji, mobbingu, zagrożenia środowiska – katalog jest szeroki. Sygnalista działający w dobrej wierze podlega ochronie nawet, jeśli okaże się, że nie było naruszenia.

PRAWDA ☐ FAŁSZ ☐

Pracodawca może zwolnić lub ukarać sygnalistę, jeśli uważa, że ten zaszkodził firmie.

PRAWDA ☐ FAŁSZ ☐

1 odpowiedź - prawda. 2 odpowiedź - prawda. 3 odpowiedź - fałsz

Quantifier.ai

MARZEC

Miesiąc cyberbezpieczeństwa

Cyberbezpieczeństwo
to codzienny nawyk,
nie jednorazowa akcja.

Miesiąc cyberbezpieczeństwa

Cyberbezpieczeństwo to kultura odpowiedzialnego korzystania z informacji, narzędzi i systemów w całej organizacji. Wraz z wejściem w życie nowych regulacji, ochrona danych i zapewnienie ciągłości działania stają się obowiązkiem prawnym, a nie tylko dobrym zwyczajem.

Z danych CERT Polska wynika, że liczba cyberataków w Polsce rośnie średnio o 25% rok do roku, co plasuje nas wśród europejskiej czołówki pod względem dynamiki zagrożeń. Najczęściej dotyczą one phishingu, ransomware oraz prób nieautoryzowanego dostępu do systemów firmowych.

Jednocześnie aż 73% organizacji przyznaje, że odczuwa rosnącą presję regulacyjną, a tylko 3% firm deklaruje, że jest w pełni przygotowana na nowoczesne wyzwania cyberbezpieczeństwa i wymogi dyrektywy NIS2.

Ataki phishingowe, wycieki danych czy złośliwe oprogramowanie mogą dziś zagrozić nie tylko reputacji, ale i funkcjonowaniu całej firmy. Dlatego marzec poświęcamy na zrozumienie, jak zbudować systemowe podejście do bezpieczeństwa informacji – zgodne z normami ISO 27001 i dyrektywami UE.

Kluczowe statystyki

29%

Z danych CERT wynika, że liczba cyberataków w Polsce wzrosła z 2023 do 2024 roku o 29%. Co plasuje nas wśród europejskiej czołówki pod względem dynamiki zagrożeń.*

3%

organizacji globalnie ma „mature” poziom gotowości na współczesne zagrożenia cyber – reszta jest w fazie początkowej lub formującej.**

Quantifier.ai

* https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie
** https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cisco-study-reveals-very-few-organizations-prepared-to-defend-against-todays-rapidly-evolving-threat-landscape.html

Najważniejsze regulacje i normy

Dyrektywa NIS2 (Network and Information Security Directive 2)

Nowa dyrektywa unijna dotycząca bezpieczeństwa sieci i systemów informatycznych, obowiązująca od 2024/2025 roku.

Jej celem jest wzmocnienie odporności organizacji na cyberzagrożenia – szczególnie w sektorach kluczowych (energia, transport, finanse, zdrowie, usługi cyfrowe).

Wymaga od firm m.in.:

- wyznaczenia odpowiedzialnych osób za cyberbezpieczeństwo,
- wprowadzenia procedur zarządzania ryzykiem i incydentami,
- raportowania poważnych incydentów w ciągu 24 godzin,
- wdrożenia planów ciągłości działania (BCP).

Podstawa prawna: Dyrektywa (UE) 2022/2555 z 14 grudnia 2022 r.

ISO 27001 – System Zarządzania Bezpieczeństwem Informacji (ISMS)

IMiędzynarodowa norma określająca, jak chronić informacje przed utratą, zniszczeniem lub nieuprawnionym dostępem.
To standard, który wdraża strukturalne podejście do cyberbezpieczeństwa — obejmujące ludzi, procesy i technologie.

Podstawowe elementy:

- polityka bezpieczeństwa informacji,
- zarządzanie ryzykiem i incydentami,
- kontrola dostępu i szyfrowanie,
- świadomość użytkowników i szkolenia,
- ciągłe doskonalenie

DLACZEGO CYBERBEZPIECZEŃSTWO JEST WAŻNE?

1

Ochrona reputacji i zaufania.
Jedno włamanie, wyciek danych czy incydent bezpieczeństwa może zniszczyć zaufanie klientów i partnerów budowane latami. W cyfrowym świecie reputacja firmy jest tak silna, jak jej zabezpieczenia.

2

Ciągłość działania
Ataki ransomware czy awarie systemów potrafią zatrzymać produkcję, sprzedaż czy obsługę klientów. Dobre praktyki cyberbezpieczeństwa minimalizują ryzyko przestoju i strat finansowych.

3

Zgodność z przepisami (compliance)
Regulacje takie jak NIS2, RODO, ISO 27001, DORA czy AI Act nakładają obowiązki dotyczące bezpieczeństwa informacji. Brak zgodności to nie tylko ryzyko kar finansowych, ale też utrata możliwości współpracy z dużymi kontrahentami czy instytucjami publicznymi.

4

Bezpieczeństwo ludzi i danych
Cyberataki często prowadzą do ujawnienia danych osobowych lub poufnych informacji. To bezpośrednio zagraża prywatności, bezpieczeństwu pracowników, klientów i całej organizacji.

5

Odpowiedzialność zarządu
Nowe przepisy, jak NIS2, przenoszą odpowiedzialność za cyberbezpieczeństwo na poziom kierownictwa. Zarząd odpowiada nie tylko finansowo, ale też wizerunkowo i prawnie za brak działań w tym obszarze.

6

Przewaga konkurencyjna
Firmy, które mogą wykazać wysoki poziom bezpieczeństwa (np. certyfikat ISO 27001), zyskują zaufanie rynku, łatwiej zdobywają kontrakty i partnerów.

Quantifier.ai

INNE NORMY I REGULACJE

Regulacja / Standard	Pełna nazwa	Opis / Zakres zastosowania
DORA	Digital Operational Resilience Act	Rozporządzenie UE (obowiązuje od 2025 r.) dotyczące odporności cyfrowej sektora finansowego. Wymaga od banków, ubezpieczycieli, funduszy i dostawców IT m.in. zarządzania ryzykiem ICT, testów penetracyjnych, raportowania incydentów i kontroli dostawców usług technologicznych (m.in. chmurowych).
Cyber Resilience Act (CRA)	Cyber Resilience Act	Rozporządzenie UE w sprawie bezpieczeństwa produktów cyfrowych i oprogramowania. Wymaga od producentów, importerów i dystrybutorów zapewnienia „security by design", zarządzania podatnościami, aktualizacji bezpieczeństwa i deklaracji zgodności CE. Obejmuje IoT, smart devices, systemy embedded i aplikacje.
CER Directive	Critical Entities Resilience Directive	Dyrektywa UE (2022/2557) o odporności podmiotów krytycznych – uzupełnienie NIS2. Obejmuje sektory: energia, transport, zdrowie, finanse, woda, administracja, infrastruktura cyfrowa. Zobowiązuje do oceny ryzyk, planów odporności i zarządzania kryzysowego.
eIDAS 2.0	Electronic Identification, Authentication and Trust Services Regulation (recast)	Nowa wersja rozporządzenia eIDAS regulująca cyfrową tożsamość i usługi zaufania w UE. Wprowadza Europejski Portfel Tożsamości Cyfrowej (EUDI Wallet), bezpieczne logowanie, podpisy elektroniczne i kwalifikowane usługi identyfikacji. Kluczowe dla bezpieczeństwa transakcji i e-administracji.
NIST Cybersecurity Framework (CSF)	NIST CSF – National Institute of Standards and Technology Cybersecurity Framework	Amerykański framework zarządzania ryzykiem cyber oparty na 5 funkcjach: Identify, Protect, Detect, Respond, Recover. Uniwersalny model używany globalnie jako praktyczny standard do oceny i budowy systemów bezpieczeństwa. Wersja 2.0 (2024) uwzględnia m.in. AI, łańcuch dostaw i governance.
EU Cybersecurity Certification Framework	Rozporządzenie (UE) 2019/881 – Cybersecurity Act	Tworzy Europejski system certyfikacji cyberbezpieczeństwa dla produktów i usług ICT, zarządzany przez ENISA. Celem jest ujednolicenie poziomów zaufania („Basic", „Substantial", „High") i promowanie bezpieczeństwa by design. Fundament dla przyszłych certyfikatów (np. cloud, 5G, IoT).

21 MARCA

PIERWSZY DZIEŃ WIOSNY

Zrób wiosenne porządki... w swoich hasłach!

Jak stworzyć dobre hasło – najważniejsze zasady

- Długość: 12–14 znaków, im dłuższe, tym lepsze.
- Różnorodność znaków: używaj dużych i małych liter, cyfr oraz symboli (!, @, $).
- Brak oczywistości: unikaj imion, dat urodzenia, nazwy firmy, prostych ciągów („123456", „qwerty").
- Unikalność: każde konto = inne hasło.
- Passphrase: twórz hasła z fraz, np. KawaZPoranka#2025 lub KotLubiKanapę!.
- Regularność: zmieniaj hasła co 6–12 miesięcy lub po incydencie bezpieczeństwa.
- Bezpieczne przechowywanie: używaj menedżera haseł
- Dodatkowe zabezpieczenie: włącz uwierzytelnianie wieloskładnikowe (MFA) wszędzie, gdzie się da.
- Nie zapisuj haseł w plikach na komputerze (plik „hasła.xlsx" to nie sejf).

31 MARCA

ŚWIATOWY DZIEŃ BACKUPU

Dzień przypomina o znaczeniu regularnego tworzenia kopii zapasowych, aby chronić dane przed utratą w wyniku awarii, kradzieży lub przypadkowego usunięcia.

Jest to dzień poświęcony edukacji o zagrożeniach związanych z utratą danych oraz promowaniu odpowiednich strategii ich zabezpieczania.

COMPLIACE BINGO

„Compliance Bingo” to narzędzie kultury zgodności, które łączy edukację, humor i codzienną refleksję nad zachowaniami w organizacji. Może funkcjonować jako materiał na szkolenie, albo gra integracyjna w zespole.

Wprowadzić lekkość do compliance. Pokaż, że przestrzeganie zasad i świadomość ryzyka nie musi być nudna. „Bingo” działa jako gamifikacja codziennych zadań, rozmów, rytuałów i wewnętrznych inside joke’ów branży regulacyjnej.

BINGO 4X4

Bingo to gra, w której uczestnicy mają planszę z różnymi hasłami lub liczbami i zaznaczają pola, gdy zostaną one „wylosowane” lub spełnione. Celem jest ułożenie pełnej linii – poziomej, pionowej lub po przekątnej – i zawołanie „Bingo!”. To prosta, zabawna forma rywalizacji, którą można wykorzystać także w edukacji lub pracy, np. do nauki o compliance.

Cytowałeś artykuł z dyrektywy z pamięci	Wysłałeś przypomnienie o szkoleniu po raz trzeci	Spotkanie „na 15 minut” trwało godzinę	Zrobiłeś prezentację o etyce z memem
Pojawił się nowy formularz od IT	Otworzyłeś nową dyrektywę i zrobiło ci się słabo	Przesłałeś „policy draft v4.1_final_fina”	Wysłano raport dzień przed deadline’em
Ktoś powiedział: „to nie nasz obszar”	Ktoś pomylił „compliance” z „complain”	Audytor zapytał: „czy macie dowód na to?”	Zrobiłeś checklistę do checklisty
Przeszedłeś szkolenie, które sam przygotowałeś	Usłyszałeś „ale przecież wszyscy tak robią”	Zrobiłeś prezentację o etyce z memem	Wysłano raport dzień po deadlinie

Dwie prawdy i jeden fałsz.

Zaznacz prawidłową odpowiedź:

	PRAWDA	FAŁSZ
Hasło „123456” nadal znajduje się w top 3 najczęściej używanych na świecie.	☐	☐
Kliknięcie w link od nieznanego nadawcy to świetny sposób na poznanie nowych ludzi.	☐	☐
Regularne aktualizacje systemu mogą uchronić przed większością cyberataków.	☐	☐

1 odpowiedź - prawda. 2 odpowiedź -fałsz. 3 odpowiedź - prawda

Quantifier.ai

Checklista cyberbezpieczeństwa

Co warto sprawdzić w marcu w Waszej firmie?

Zarządzanie i odpowiedzialność

- Czy wyznaczono oficera ds. bezpieczeństwa informacji / CISO?
- Czy zarząd jest regularnie informowany o ryzykach i incydentach cyber?
- Czy istnieje strategia / polityka bezpieczeństwa informacji (ISMS) zatwierdzona przez kierownictwo?
- Czy obowiązki w zakresie cyberbezpieczeństwa są przypisane do konkretnych ról (np. IT, HR, Operations)?
- Czy jest prowadzony rejestr aktywów informacyjnych (systemy, dane, dostawcy)?

- **Kontrola dostępu i tożsamości (Access & Identity Management)**

- Czy wszyscy użytkownicy mają unikalne konta (brak współdzielonych loginów)?
- Czy obowiązuje zasada najmniejszych uprawnień (Least Privilege Principle)?
- Czy stosowane jest uwierzytelnianie wieloskładnikowe (MFA)?
- Czy procedura nadawania i odbierania dostępu działa automatycznie przy zatrudnieniu/odejściu pracowników?

Infrastruktura i systemy IT

- Czy oprogramowanie pochodzi wyłącznie z autoryzowanych źródeł?
- Czy istnieją kopie zapasowe (backup) — testowane i przechowywane offline?
- Czy serwery i urządzenia końcowe mają aktualne oprogramowanie antywirusowe?
- Czy sieć firmowa jest segmentowana (np. oddzielone sieci biurowe, gościnne)?
- Czy jest wdrożony firewall / IDS / IPS i monitoring ruchu sieciowego?

Czy wiesz, że... ?
Zasada najmniejszych uprawnień mówi, że każdy użytkownik, proces, system lub aplikacja powinien mieć dostęp tylko do tych zasobów, które są niezbędne do wykonania jego bieżących zadań – i nic więcej.

Checklista cyberbezpieczeństwa

Co warto sprawdzić w marcu w Waszej firmie?

Zarządzanie dostawcami

- Czy prowadzony jest rejestr dostawców mających dostęp do danych lub systemów?
- Czy każdy dostawca przeszedł ocenę ryzyka / due diligence (certyfikat, ankieta, audyt)?
- Czy umowy zawierają klauzule bezpieczeństwa i incydentów?
- Czy dostawcy podlegają okresowym przeglądom zgodności?
- Czy istnieje plan awaryjny na wypadek awarii lub ataku u dostawcy?

Zarządzanie incydentami i kryzysami

- Czy jest wdrożona Polityka zarządzania incydentami?
- Czy istnieje dedykowany zespół reagowania lub zewnętrzny partner?
- Czy pracownicy wiedzą, jak i komu zgłaszać incydent?

Zarządzanie ryzykiem i audyty

- Czy prowadzony jest rejestr ryzyk cyberbezpieczeństwa?
- Czy regularnie przeprowadzane są oceny ryzyka?
- Czy zidentyfikowano kluczowe aktywa i systemy krytyczne?
- Czy realizowane są audyt wewnętrzny / testy penetracyjne?
- Czy wnioski z audytów są dokumentowane i wdrażane?

Ciągłość działania i Disaster Recovery

- Czy organizacja posiada Plan Ciągłości Działania, który określa, jak utrzymać kluczowe procesy w razie awarii lub kryzysu?
- Czy najważniejsze systemy i dane mają kopie zapasowe przechowywane w innej lokalizacji lub w chmurze?
- Czy określono maksymalny dopuszczalny czas przestoju (RTO) oraz poziom utraty danych (RPO), czyli jak szybko i z jaką dokładnością dane muszą zostać przywrócone po awarii?

Szkolenia i świadomość użytkowników

- Czy każdy pracownik przeszedł szkolenie z cyberbezpieczeństwa?

KWIECIEŃ

Miesiąc środowiskowy: ślad węglowy, Paszport Produktowy i cyrkularność

Nasza planeta, nasz biznes – compliance środowiskowy jako inwestycja w przyszłość.

Miesiąc środowiskowy: ślad węglowy, Paszport Produktowy, cyrkularność

Kwiecień, w którym obchodzimy Dzień Ziemi (22 kwietnia), to idealny moment, by spojrzeć na nasze obowiązki środowiskowe. Przepisy z obszaru EHS (Environment, Health & Safety – środowisko, zdrowie i bezpieczeństwo) oraz ESG (Environmental, Social & Governance – środowisko, kwestie społeczne i ład korporacyjny) rozwijają się równie szybko, jak rośnie świadomość klimatyczna.

Firmy muszą mierzyć swój ślad węglowy GHG (Greenhouse Gas – emisje gazów cieplarnianych), dbać o efektywność energetyczną i bezpieczeństwo pracy. Pomagają w tym m.in. ISO 14001 (system zarządzania środowiskowego) i ISO 45001 (system zarządzania bezpieczeństwem i higieną pracy). W Unii Europejskiej nadchodzą też nowe wymagania, takie jak cyfrowy paszport produktowy — zestaw kluczowych informacji o wpływie produktu na środowisko — oraz ESRS (European Sustainability Reporting Standards), czyli europejskie standardy raportowania zrównoważonego rozwoju.

W ramach dyrektywy CSRD (Corporate Sustainability Reporting Directive) już od 2025 r. duże firmy w UE będą raportować zgodnie z modułem ESRS E, obejmującym m.in. emisje GHG, zużycie zasobów czy bioróżnorodność. To ogromna zmiana: liczba firm objętych raportowaniem wzrośnie z ok. 11 700 do niemal 50 000.
Tymczasem globalne emisje w 2022 r. osiągnęły rekordowe 57,4 gigatony CO_2e. Naukowcy ostrzegają, że bez szybkich redukcji do 2030 roku nie utrzymamy ocieplenia na bezpiecznym poziomie. Nic więc dziwnego, że polityki klimatyczne — jak unijny pakiet Fit for 55 zakładający redukcję emisji o 55% do 2030 r. i neutralność klimatyczną do 2050 r. — stawiają przed firmami coraz większe wymagania.Dla biznesu oznacza to konieczność systemowego podejścia: od pomiaru emisji (w tym trudnego Scope 3 — emisje pośrednie w łańcuchu dostaw), przez plany redukcji, aż po odpowiedzialne działania kompensacyjne. Dzisiejsze compliance środowiskowe staje się równie ważne jak finansowe — bo zaniedbania grożą nie tylko karami, ale także utratą zaufania inwestorów, klientów, a nawet finansowania dla firm wysokoemisyjnych.

Kluczowe statystyki

57,4 Gt CO_2e
rekordowe globalne emisje gazów cieplarnianych w 2022 (1990: ~37 Gt, wzrost o 55%).*

7%,
tyle dużych firm mierzy pełne emisje Scope 1–3, reszta nie zna w pełni swoich emisji bezpośrednich i pośrednich.**

300 410:
liczba organizacji z ISO 14001 w 2022. Dla porównania ISO 50001 (energia) ma ~24 924 firm.***

Quantifier.ai

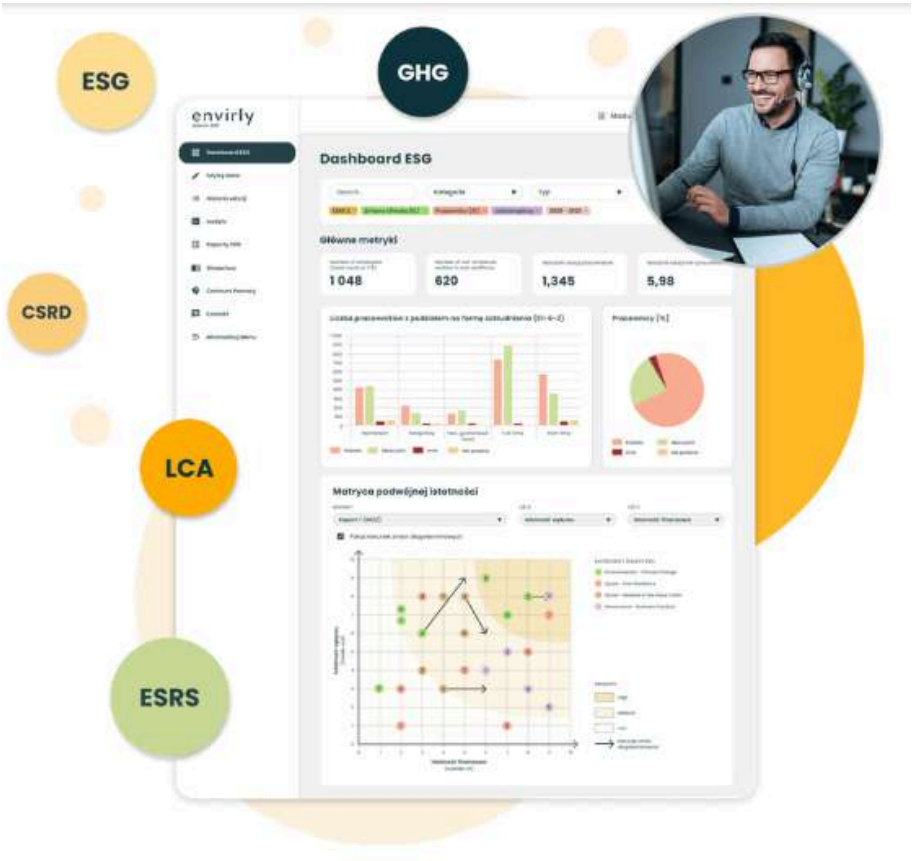
* https://www.unep.org/interactives/emissions-gap-report/2023/#section_-1
** https://www.co2ai.com/climate-survey-2025
*** https://certiget.eu/en/guides/iso-survey-2023-report-results-global-trends-in-iso-management-systems-certification

Case study: Automatyzacja zarządzania środowiskowego

W obliczu rosnących wymogów środowiskowych jedna z firm produkcyjnych postanowiła pójść o krok dalej i wdrożyć platformę Envirly by Quantifier, moduł ESG, która automatyzuje zbieranie danych, liczenie emisji i kontrolę zgodności. Zamiast ręcznego zbierania informacji z działów, dane zaczęły spływać do systemu same, z liczników energii, systemu ERP oraz ankiet wysyłanych do dostawców.

Platforma automatycznie oblicza emisje Zakres 1 i Zakres 2, a także zbiera informacje potrzebne do szacowania Zakres 3: od emisji u dostawców materiałów, przez transport, po użytkowanie produktów przez klientów. Menedżerowie mogą w czasie rzeczywistym śledzić emisje na jednostkę produkcji i sprawdzać, czy firma mieści się w zakładanych celach redukcyjnych.

Wykorzystano także moduł Envirly by Quantifier, moduł ESG, Paszportowy Paszport: platforma gromadzi dane o składzie materiałowym produktów, udziale recyklingu i możliwości ponownego przetworzenia. Firma dzięki temu przygotowuje się do nadchodzących przepisów wprowadzających cyfrowe paszporty produktów.



Quantifier.ai

Lista kontrolna - compliance środowisko i BHP:

1. Czy mierzymy nasz ślad węglowy (emisje CO_2 i ekwiwalent innych gazów)? – Jeśli jeszcze nie, czas zacząć choćby od Scope 1+2. Jeśli tak, czy uwzględniamy także Scope 3 (dostawcy, transport, użytkownicy produktów)? (To trudne, ale łańcuch dostaw to często >70% emisji firmy).

2. Czy posiadamy aktualną Politykę Środowiskową i/lub Klimatyczną firmy, zatwierdzoną przez zarząd? – Czy zawiera cele (np. redukcji emisji, ograniczenia odpadów) i czy są one mierzalne i przeglądane regularnie?

3. Czy wdrożyliśmy system zarządzania wg ISO 14001 (środowisko) lub ISO 50001 (energia) – albo chociaż elementy tych standardów? – Np. cykl PDCA dla aspektów środowiskowych, regularne przeglądy zgodności z przepisami (compliance audit), monitoring zużycia mediów.

4. Paszport produktowy: Czy wiemy, jakie informacje o naszych produktach mogą być wymagane w przyszłości? – Np. ślad węglowy produktu, materiały niebezpieczne, możliwości recyklingu. Już teraz warto zacząć zbierać te dane, by nie robić tego w panice w ostatniej chwili.

5. ESRS/CSRD: Czy nasza firma (lub grupa kapitałowa) będzie objęta raportowaniem zrównoważonego rozwoju według nowych standardów? – Kryteria to m.in. >250 pracowników i >40 mln € obrotu. Jeśli tak, czy mamy zespół projektowy i plan zbierania danych ESG za 2025 rok? (Pierwsze raporty dla największych firm już w 2025 za rok 2024).

6. Zgodność z przepisami lokalnymi: Czy spełniamy bieżące obowiązki: pozwolenia emisyjne, opłaty środowiskowe, sprawozdawczość (KOBiZE, BDO – odpady, F-gazy itd.)? – Upewnij się, że terminy nie są przekraczane, a dokumentacja jest aktualna.

7. ISO 45001 (BHP): Czy posiadamy system zarządzania bezpieczeństwem pracy? – Sprawdź, czy prowadzimy oceny ryzyka zawodowego, szkolenia BHP, czy zgłaszamy i analizujemy wypadki oraz incydenty. Kwiecień to dobry moment na przegląd procedur przed majowym Dniem BHP.

8. Energia: Czy monitorujemy zużycie energii i realizujemy audyt energetyczny co 4 lata (jeśli wymagany przez prawo dla dużych firm)? – Oszczędność energii to teraz nie tylko kwestia kosztów, ale i emisji (mniej kWh = mniej CO_2).

9. Dostawcy: Czy w umowach z dostawcami/wykonawcami mamy klauzule zobowiązujące ich do przestrzegania prawa środowiskowego i BHP? – Warto też mieć proces weryfikacji dostawców pod tym kątem (np. czy nie mieli poważnych sankcji środowiskowych).

22 KWIETNIA

MIĘDZYNARODOWY DZIEŃ ZIEMI

Obchodzony od 1970 r., obecnie globalne święto ekologii. W firmach to często okazja do akcji wolontariackich (sadzenie drzew, sprzątanie świata) oraz kampanii edukacyjnych.

Można tego dnia ogłosić nowe zobowiązanie środowiskowe firmy – np. cel redukcji plastiku jednorazowego, dołączenie do Science Based Targets lub opublikowanie Polityki Klimatycznej.

Pogromcy mitów. Mity o zgodności środowiskowej

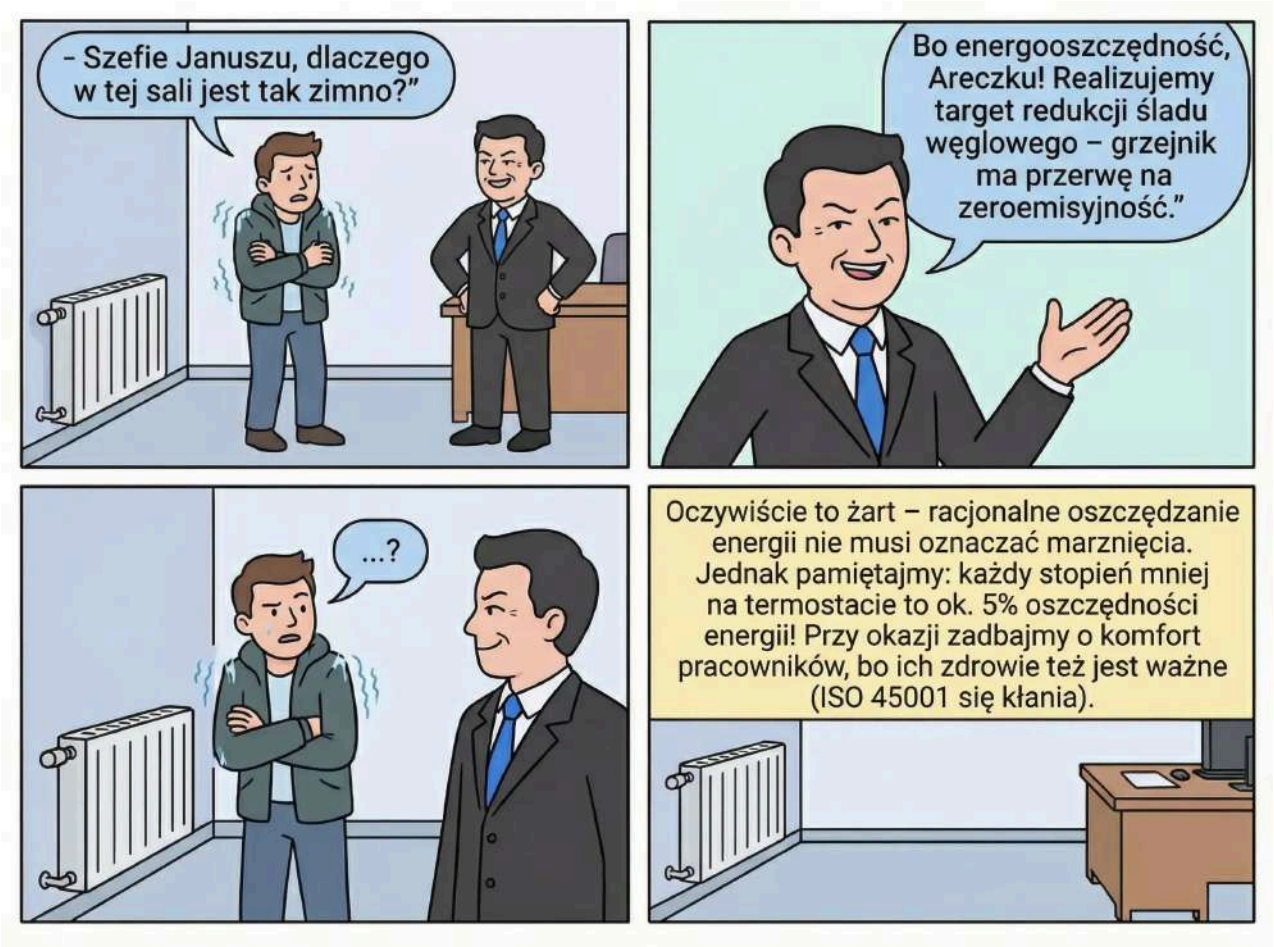
- **Mit**: „Ekologia w biznesie to tylko marketing (greenwashing), realnie mało kto się tym przejmuje, bo to kosztuje."
- **Fakt**: Coraz więcej twardych regulacji wymusza prośrodowiskowe działania – od systemu EU ETS (prawa do emisji CO_2) po normy efektywności energetycznej dla budynków i urządzeń. Koszty braku ekologii rosną (opłaty, kary, bojkoty konsumenckie), a badania pokazują, że firmy wdrażające zrównoważone praktyki często zyskują w długim terminie dzięki oszczędnościom i lojalności klientów. Greenwashing zaś grozi poważnymi sankcjami – np. UE pracuje nad dyrektywą zakazującą fałszywych eko-claimów. Biznes musi traktować ekologię serio, bo inaczej wypadnie z gry.

- **Mit**: „Certyfikat ISO 14001 czy raport ESG oznacza, że firma jest ekologiczna."
- **Fakt**: Certyfikaty i raporty to narzędzia, które świadczą o tym, że firma zarządza swoim wpływem na środowisko i go monitoruje, ale nie gwarantują perfekcyjnych wyników. ISO 14001 wymaga ciągłego doskonalenia – nawet firmy z certyfikatem mogą mieć incydenty, jeśli nie pilnują tematu. Raport ESG może wyglądać ładnie, ale ważna jest wiarygodność danych. Dlatego tak istotny jest audyt i weryfikacja (np. zewnętrzne assurance dla raportów ESG). Podsumowując: certyfikat/raport to nie zwolnienie z myślenia – to zobowiązanie do stałej poprawy.

Wyzwanie na kwiecień

Zorganizuj firmowy Dzień Ziemi (22 IV) – np. akcję sprzątania okolicy biura lub konkurs na pomysł ekologicznej inicjatywy w firmie. W skali całego miesiąca: zmniejszcie zużycie papieru o 10% (prowadząc kampanię “PaperLess April”), albo zasadźcie drzewo za każdy zrealizowany cel kwartalny. Możecie też przeprowadzić audyt energetyczny mini-skali – np. sprawdzić, gdzie niepotrzebnie działają urządzenia w trybie czuwania i wprowadzić dobre nawyki (wyłączanie monitorów, oświetlenia po godzinach).

Dla chętnych: spróbuj policzyć ślad węglowy wybranego projektu lub produktu Waszej firmy – potraktujcie to jako pilotaż przed pełnym obowiązkiem raportowania. Kluczowe jest zaangażowanie ludzi – niech poczują, że troska o planetę jest wspólną misją, a nie tylko odgórnym nakazem.



Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

Norma ISO 14001 (system zarządzania środowiskowego) jest dobrowolna, ale jej wdrożenie pomaga w spełnieniu wymogów prawnych i ograniczaniu ryzyk środowiskowych.

PRAWDA ☐ **FAŁSZ** ☐

Wiele przedsiębiorstw odkrywa, że nawet 80–90% ich całkowitych emisji CO_2 pochodzi z zakresu 3 (łańcuch dostaw, użycie produktów).

PRAWDA ☐ **FAŁSZ** ☐

Tylko firmy z branży energetycznej czy ciężkiego przemysłu muszą przejmować się raportowaniem emisji – reszta może spać spokojnie.

PRAWDA ☐ **FAŁSZ** ☐

1 odpowiedź - prawda. 2 odpowiedź prawda. 3 odpowiedź - fałsz

Quantifier.ai

MAJ

Miesiąc antykorupcji i ładu korporacyjnego

Gramy fair – zero tolerancji dla korupcji, etyka fundamentem ładu korporacyjnego.

Miesiąc antykorupcji i ładu korporacyjnego

W maju kierujemy uwagę na przeciwdziałanie korupcji oraz ład korporacyjny (corporate governance). 19 maja obchodzony jest Światowy Dzień Fair Play, który w sporcie promuje uczciwość – w biznesie przekłada się to na etykę i przejrzystość w działalności gospodarczej. Korupcja pozostaje jednym z największych problemów globalnej gospodarki: ONZ i Światowe Forum Ekonomiczne szacują, że pochłania ok. 5% światowego PKB, czyli ok. 5 bln dolarów rocznie – równowartość rocznego PKB Japonii. W krajach rozwijających się straty sięgają ok. 1,26 bln dolarów rocznie, co mogłoby wyciągnąć z biedy 1,4 mld ludzi na 6 lat. Nic dziwnego, że rządy zaostrzają regulacje: funkcjonują surowe ustawy antykorupcyjne jak amerykańska FCPA, brytyjski UK Bribery Act czy francuska Sapin II, o zasięgu eksterytorialnym, a w Polsce – ustawa o odpowiedzialności podmiotów zbiorowych, przewidująca dotkliwe kary i zakazy. Coraz częściej standardem staje się posiadanie przez firmy programów antykorupcyjnych, czego odzwierciedleniem są m.in. normy typu ISO 37001 (System Zarządzania Przeciwdziałaniem Korupcji). Maj to dobry moment, by sprawdzić, czy nasze organizacje rzeczywiście mają się czym wykazać w obszarze compliance antykorupcyjnego i etycznego ładu – rozumianego nie tylko jako formalne struktury (rady nadzorcze, komitety audytu), lecz przede wszystkim jako kultura organizacyjna promująca uczciwość, przejrzystość i rozliczalność.

Kluczowe statystyki

5% PKB

szacowany koszt korupcji dla globalnej gospodarki (ponad 5 bln $ rocznie).*

ok. 43%

przypadków nadużyć – wykrywane dzięki sygnalistom. Dla porównania audyt wewnętrzny wykrywa tylko 14%, a organy ścigania <2%.**

Quantifier.ai

* https://www.unodc.org/corruption/en/index.html
** https://legacy.acfe.com/report-to-the-nations/2024/

Case study: Firma bez korupcji – jak system może pomóc.

Spółka handlowa działa w krajach o podwyższonym ryzyku korupcji. Firma wiedziała, że tradycyjne procedury to za mało, potrzebowała systemu, który realnie wychwyci sygnały ostrzegawcze, zanim przerodzą się w poważny problem. Dlatego wdrożono platformę Quantifier.

- Wprowadzono elektroniczny rejestr prezentów i zaproszeń (wszystko powyżej 50 € trafia automatycznie do systemu), a każde przekroczenie limitu natychmiast wywołuje alert do compliance.
- Uruchomiono moduł due diligence kontrahentów: kwestionariusze ryzyka przed podpisaniem umowy, automatyczne rekomendacje i jasna dokumentacja decyzji biznesowych.
- Do tego dochodzi platforma e-learningowa, na której wszyscy pracownicy przechodzą coroczne szkolenia i testy z etyki oraz antykorupcji. System monitoruje ukończenia, wysyła przypomnienia i tworzy pełną ścieżkę audytową. Firma regularnie prowadzi też ankiety w działach sprzedaży i zakupów, badając realne przypadki prób nacisku, nieformalnych „prowizji" czy konfliktów interesów.

Efekty, które szybko stały się widoczne

- W pierwszym roku wykryto dwóch pośredników o podwyższonym ryzyku – współpraca została natychmiast zakończona.
- Zgłoszono kilka incydentów, w tym nieformalne propozycje zapłaty za „przyspieszenie procesu".
- Z jednym dostawcą rozwiązano umowę, chroniąc firmę przed poważnymi konsekwencjami regulacyjnymi.
- Wiedza pracowników wzrosła spektakularnie: 100% badanych zna procedurę zgłaszania korupcji (wcześniej ok. 60%).

Czy wiesz że....

W części jurysdykcji wprowadzono już prawny obowiązek posiadania systemu antykorupcyjnego – przykładem jest francuska ustawa Sapin II, która nakłada na duże firmy obowiązek wdrożenia programu compliance pod nadzorem Agence française anticorruption (AFA).

Lista kontrolna – antykorupcja i governance:

1. Czy mamy zdefiniowaną, wdrożoną i komunikowaną Politykę Antykorupcyjną / Etyczną? – Sprawdź, czy jest ona dostępna dla wszystkich (intranet, tablice) i zrozumiała (przykłady dopuszczalnych i niedopuszczalnych zachowań).

2. Kodeks Postępowania: Czy nasz kodeks etyki zawiera zapisy o zakazie przekupstwa, konfliktach interesów, uczciwości w raportowaniu? Czy każdy pracownik i partner podpisuje zobowiązanie do przestrzegania kodeksu?

3. Szkolenia: Czy prowadzimy regularne szkolenia z przeciwdziałania korupcji dla pracowników, zwłaszcza tych na stanowiskach wrażliwych (dział zakupów, sprzedaż, public procurement)? – Upewnij się, że nowi pracownicy są szkoleni od razu po zatrudnieniu.

4. Kanały zgłaszania nadużyć: Czy dostępny jest poufny kanał do zgłaszania podejrzeń korupcji (może to być ten sam system co dla whistleblowerów)? I czy ludzie o nim wiedzą (przypomnijmy przy okazji Dnia Fair Play)?

5. Rejestr korzyści: Czy prowadzimy rejestr otrzymywanych prezentów, zaproszeń, donacji, sponsoringu itp.? – Dobrą praktyką jest transparentność: np. publikacja raz w roku zestawienia, co firma (lub jej pracownicy) otrzymali od kontrahentów. Jeśli cokolwiek wzbudza wątpliwości – lepiej odmówić przyjęcia.

6. Due diligence stron trzecich: Czy mamy proces weryfikacji pośredników, agentów, dostawców pod kątem ryzyka korupcji? – Np. listy sankcyjne, beneficjenci rzeczywiści, reputacja. W krajach wysokiego ryzyka może to wymagać głębszej analizy.

7. Procedury kontroli: Czy w kluczowych procesach mamy mechanizmy “czterech oczu” lub rotację obowiązków? – Np. duże wydatki zatwierdzone przez więcej niż jedną osobę, rozdział funkcji zakupowych i zatwierdzających płatność. To utrudnia korupcję wewnętrzną.

8. Raportowanie i nadzór: Czy zarząd/rada nadzorcza otrzymuje regularnie raporty o stanie compliance etycznego? – Powinna istnieć metryka (KPI) np. liczba zgłoszonych incydentów, liczba przeszkolonych pracowników, wyniki audytów wewnętrznych w tym obszarze. Governance to także struktura – czy mamy oficera ds. zgodności/etyki i czy ma on autonomię oraz wsparcie zarządu?

9. Plan reakcji: Czy posiadamy gotowy plan postępowania na wypadek wykrycia przypadku korupcji lub poważnego naruszenia etyki? – Musi obejmować dochodzenie wewnętrzne, ewentualne kroki prawne, komunikację (wew/zew) i działania naprawcze. Czas reakcji jest kluczowy, bo często liczy się współpraca z organami (np. w modelu self-disclosure można złagodzić karę).

19 MAJA

WORLD FAIR PLAY DAY

Światowy Dzień Fair Play to coroczne międzynarodowe święto obchodzone 19 maja, którego celem jest promowanie wartości fair play w sporcie, takich jak uczciwość, szacunek i integralność. Dzień ten został oficjalnie ustanowiony przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych.

Pogromcy mitów. Mity o korupcji i ładzie korporacyjnym

- **Mit**: „Mała „wdzięczność" nikomu nie szkodzi – przecież wszyscy tak robią, by przyspieszyć sprawy."
- **Fakt**: Tzw. drobna korupcja (np. dawanie prezentów urzędnikom za szybsze załatwienie sprawy) jest równie nielegalna jak ta na najwyższych szczeblach. Poza tym tworzy niebezpieczny precedens – apetyt rośnie w miarę jedzenia. Drobna łapówka dziś może jutro przerodzić się w wymuszanie większych kwot. A w firmie – skoro akceptujemy małe oszustwa, to sygnał, że duże też przejdą. Zero tolerancji to jedyna słuszna droga.

- **Mit**: „Nasz biznes jest lokalny/rodzinny – nie potrzebujemy formalnego ładu korporacyjnego jak wielkie spółki."
- **Fakt**: Dobre praktyki zarządcze przydają się każdej organizacji. Jasny podział ról, etyczne wartości, mechanizmy kontroli wewnętrznej – to wszystko chroni firmę niezależnie od jej skali. W mniejszych podmiotach może nie być rozbudowanej rady nadzorczej, ale zasady accountability (rozliczalności) i tak warto wdrożyć. Np. choćby kwartalne przeglądy finansów z udziałem właścicieli i zewnętrznego doradcy, kodeks etyki rodzinnej firmy, polityka nepotyzmu itd. Im wcześniej zbudujesz ład, tym łatwiej rosnąć bez chaosu.

Wyzwanie na maj

Ogłoś wewnętrznie Tydzień Fair Play (okolice 19 maja). Każdego dnia podziel się z pracownikami jedną krótką historią związaną z etyką biznesu (może być case z gazety o firmie ukaranej za korupcję, albo przykład sportowca, który oddał medal bo wygrał nieuczciwie – inspiracja do dyskusji). Zaproś pracowników do quizu etycznego– np. w formie ankiety online z pytaniami typu: "Czy przyjęcie butelki wina od dostawcy to już naruszenie czy jeszcze dopuszczalne?". Nagrodą niech będzie symboliczny tytuł "Etycznego Mistrza Miesiąca". Równocześnie zachęć działy do zgłaszania pomysłów na usprawnienie ładu korporacyjnego – np. lepszy przepływ informacji do rady nadzorczej, albo nowe kanały komunikacji z pracownikami (ład korporacyjny to także przejrzystość i dialog!). W maju warto też przejrzeć rejestr korzyści z ostatniego roku – czy coś budzi wątpliwości? Jeśli tak, podejmij działania wyjaśniające teraz, zanim sprawa urośnie.

Dwie prawdy i jeden fałsz.

Zaznacz prawidłową odpowiedź:

Wręczenie lub przyjęcie łapówki to przestępstwo w prawie większości krajów – zarówno ten, kto daje, jak i ten, kto bierze, podlega karze.

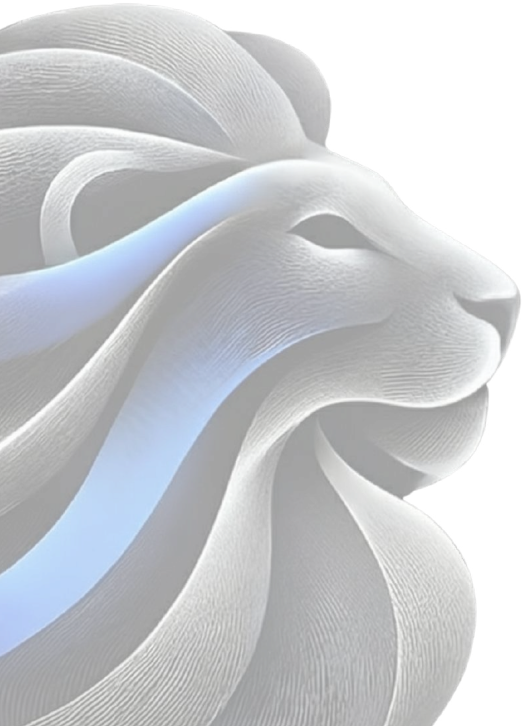
PRAWDA ☐ **FAŁSZ** ☐

Wdrożenie polityki antykorupcyjnej i jednorazowe szkolenie pracowników gwarantuje, że firma nie będzie mieć problemów z korupcją.

PRAWDA ☐ **FAŁSZ** ☐

Tzw. „facilitation payments" – drobne płatności przyspieszające rutynowe czynności urzędowe – są nielegalne w wielu jurysdykcjach (np. w Wielkiej Brytanii absolutnie zakazane przez UK Bribery Act).

PRAWDA ☐ **FAŁSZ** ☐



1 odpowiedź - prawda. 2 odpowiedź fałsz. 3 odpowiedź - prawda

Quantifier.ai

CZERWIEC

Miesiąc ryzyka i compliance

Brak ryzyka lubi porządek.

Miesiąc ryzyka i compliance

Compliance nie istnieje bez ryzyka – a ryzyko bez nadzoru zamienia się w chaos. Zarządzanie ryzykiem to codzienna umiejętność przewidywania, gdzie w organizacji coś może pójść nie tak — zanim faktycznie pójdzie.
W praktyce oznacza to identyfikowanie zagrożeń (np. korupcja, greenwashing, błędne raportowanie danych ESG), ocenę ich wpływu oraz wdrażanie działań kontrolnych.
Dobrze zaprojektowany system zarządzania ryzykiem pomaga nie tylko spełniać wymogi regulacyjne, ale też podejmować lepsze decyzje biznesowe i chronić reputację organizacji.

Podstawowe ramy, które pomagają to uporządkować:

- ISO 31000 – Risk Management Standard – uniwersalne podejście do identyfikacji, oceny i reagowania na ryzyko (także w compliance).
- COSO ERM Framework – klasyk wykorzystywany w sektorze finansowym, łączący ryzyka strategiczne, finansowe i operacyjne.
- ESRS 2 – IRO-1 (CSRD) – wymaga formalnego udokumentowania procesu identyfikacji i oceny ryzyk ESG, dlatego mapa ryzyk coraz częściej staje się częścią raportu niefinansowego.

Kluczowe statystyki

16,2 mln USD
średni roczny koszt incydentów związanych z ryzykiem wewnętrznym na organizację (wzrost z 15,4 mln rok wcześniej)*

88%
organizacji przeznacza mniej niż 10% budżetu bezpieczeństwa IT na zarządzanie ryzykiem wewnętrznym (średnio ok. 8,2%)**

86 dni
średni czas potrzebny na opanowanie incydentu insiderskiego (2023)***

Quantifier.ai

* https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/
** https://www.reveal.security/wp-content/uploads/rs-whitepaper-insider-threats-071224.pdf
*** https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/

Lista kontrolna

1. Zaktualizuj rejestr ryzyk compliance i ESG – przynajmniej raz na pół roku.
2. Przelicz scoring (prawdopodobieństwo × wpływ) i sprawdź, które ryzyka „urosły".
3. Sprawdź, czy Twoje ryzyka są powiązane z właścicielami procesów (Finance, HR, IT).
4. Zaplanuj spotkanie z zarządem w formacie Top 5 risk highlights – jedno slajdowe podsumowanie.
5. Ustal, które ryzyka możesz monitorować automatycznie w systemie.

Czy wiesz że....

Pierwsze oficjalne mapy ryzyk w historii tworzono w 1970 r. w NASA po katastrofie Apollo 13. To wtedy powstało powiedzenie: „Planowanie ryzyka to planowanie sukcesu."

5 CZERWCA

ŚWIATOWY DZIEŃ BEZPIECZEŃSTWA ŻYWNOŚCI

Zwany też jako Światowy Dzień Środowiska (World Environment Day WED), obchodzony jest corocznie 5 czerwca. Dzień ten został ustanowiony przez Zgromadzenie Ogólne ONZ na Konferencji Sztokholmskiej w 1972 roku i obchodzony jest dla przypomnienia głównych haseł konferencji dotyczących zgodności rozwoju cywilizacji z rozwojem ekologicznym otaczającego świata. Konferencja Sztokholmska doprowadziła do ustanowienia programu ONZ dedykowanego środowisku naturalnemu człowieka, określanego jako Program Środowiskowy Organizacji Narodów Zjednoczonych (UN Environment).

Pogromcy mitów:

Mit: Jeśli nic się nie wydarzyło, ryzyka nie ma.
Fakt: Ryzyko nie znika, gdy go nie mierzymy – po prostu wymyka się spod radaru.

Dwie prawdy i jeden fałsz.

Zaznacz prawidłową odpowiedź:

	PRAWDA	FAŁSZ
Każda firma ma ryzyka reputacyjne.	☐	☐
Każde ryzyko można wyeliminować.	☐	☐
Ryzyko bez właściciela nie istnieje.	☐	☐

1 odpowiedź - prawda. 2 odpowiedź fałsz. 3 odpowiedź - prawda

Quantifier.ai

LIPIEC

Miesiąc normy ISO 22031 i ciągłości działania

Gdy coś musi pójść źle, niech przynajmniej Twoja organizacja będzie na to gotowa – ISO 22301 to instrukcja przetrwania, a nie zbędna formalność.

Miesiąc ISO 22031

Lipiec poświęcamy normie ISO 22301, czyli systemowemu zarządzaniu ciągłością działania. To standard, który pomaga zbudować spójny Business Continuity Management System (BCMS): od analizy ryzyka i wpływu zakłóceń, przez plany awaryjne, po testy i doskonalenie.

W świecie, w którym przerwy w dostawach, cyberataki, awarie IT i ekstremalne zjawiska pogodowe stały się codziennością, pytanie nie brzmi już „czy coś się wydarzy?", ale „jak szybko wrócimy do normalnego działania". ISO 22301 porządkuje ten chaos: wymusza zidentyfikowanie krytycznych procesów, zasobów i dostawców, zdefiniowanie poziomów RTO/RPO oraz zaplanowanie reakcji na różne scenariusze przerw.

Dobrze wdrożony system ciągłości to nie tylko „papier dla audytora", ale realna przewaga konkurencyjna: krótsze przestoje, mniejsze straty, większe zaufanie klientów i partnerów. Lipiec to dobry moment, żeby sprawdzić, czy Twój plan ciągłości to żyjący dokument, czy plik zapomniany w SharePoincie.

Kluczowe statystyki

43,6%
organizacji doświadczyło w 2024 r. zakłóceń w łańcuchu dostaw spowodowanych awarią podmiotów trzecich.*

90%
średnich i dużych firm szacuje koszt godziny przestoju IT na ponad 300 000 USD, a w części organizacji sięga on nawet miliona dolarów za godzinę.**

* https://www.thebci.org/news/supply-chain-disruptions-drive-increased-tier-mapping-and-insurance-uptake.html
** https://goleadingit.com/blog/chicago-it-downtime-real-costs-and-solutions-for-businesses/

Case study. Jak ISO 22301 uratowało ciągłość działania producenta

Producent z branży FMCG działał w modelu „just-in-time" i był uzależniony od jednego kluczowego dostawcy. Przerwa w dostawach oznaczała zatrzymanie linii produkcyjnej w kilka godzin. W ramach wdrożenia ISO 22301 firma zrobiła analizę BIA, wskazała procesy krytyczne, zdefiniowała RTO/RPO, podpisała umowy z alternatywnymi dostawcami i przygotowała procedury przełączenia produkcji.

Gdy u głównego dostawcy doszło do poważnej awarii, uruchomiono plan ciągłości: aktywowano dostawcę zapasowego, przeplanowano produkcję i wykorzystano gotowe scenariusze komunikacji z kluczowymi klientami. Przestój ograniczono do kilku godzin, a realizacja zamówień pozostała na stabilnym poziomie. Wniosek: formalny BCMS to realna różnica między „stoimy przez tydzień" a „mamy kontrolowany incydent".*

Czy wiesz że....

- Według danych cytowanych przez FEMA, 90% firm pozbawionych planu ciągłości działania upada w ciągu roku od poważnej katastrofy, co pokazuje, że brak przygotowania to nie tylko „ryzyko", ale często początek końca biznesu.
- Koszt godziny przestoju w dużej fabryce motoryzacyjnej szacuje się dziś na ok. 2,3 mln USD – każda minuta bezczynnych linii produkcyjnych to setki dolarów straty.

Te liczby dobrze pokazują, że inwestycja w ISO 22301 i BCMS nie jest „kosztem administracyjnym", tylko polisą na przetrwanie.

*Przykład jest wymyślony

Lista kontrolna - Ciągłość działania

1. **Mapa procesów krytycznych:** Czy masz zidentyfikowane i opisane procesy, których zatrzymanie najbardziej uderza w biznes (przychody, bezpieczeństwo, kluczowi klienci)?

2. **Aktualna analiza BIA i ryzyk:** Czy przeprowadzono Business Impact Analysis i ocenę ryzyk w ciągu ostatnich 12–24 miesięcy, uwzględniając nowych dostawców, systemy i lokalizacje?

3. **Zdefiniowane RTO i RPO:** Czy dla kluczowych systemów i procesów określono docelowe czasy odtworzenia (RTO) i dopuszczalną utratę danych (RPO) oraz czy IT i biznes faktycznie znają te wartości?

4. **Plany ciągłości i odtwarzania IT:** Czy istnieją spójne, udokumentowane i łatwo dostępne plany ciągłości biznesowej oraz Disaster Recovery (DR), obejmujące także kluczowych dostawców i partnerów?

5. **Testy i ćwiczenia:** Czy w ostatnim roku przeprowadzono choć jedno ćwiczenie scenariuszowe (table-top) oraz test techniczny (np. odtworzenie systemu z backupu, symulacja awarii dostawcy)?

6. **Zarządzanie dostawcami krytycznymi:** Czy posiadasz listę dostawców krytycznych, ocenę ich ryzyka oraz zapisy dot. ciągłości działania w umowach (SLA, gwarantowane czasy reakcji, plany awaryjne)?

16 LIPCA
DZIEŃ DOCENIANIA AI

Celem tego dnia jest podkreślenie, jak sztuczna inteligencja (AI) zmienia nasze życie i funkcjonowanie różnych sektorów – od ochrony zdrowia po świat biznesu – oraz docenienie jej znaczenia dla rozwoju innowacji i podnoszenia efektywności. To także moment, by zatrzymać się na chwilę, podsumować dotychczasowy postęp, porozmawiać o przyszłości i możliwościach AI, a jednocześnie zmierzyć się z wyzwaniami, jakie ze sobą niesie, w tym w obszarze etyki i cyberbezpieczeństwa.

Wyzwanie na lipiec

Lipcowe wyzwanie: „Crash test" ciągłości działania

1. Wybierz jeden krytyczny proces (np. obsługa zamówień, produkcja, logistyka, kluczowy system IT).
2. Załóż scenariusz: brak głównego dostawcy / awaria kluczowego systemu / brak dostępu do siedziby.
3. Sprawdź, czy:
   - masz aktualny plan działania na taki scenariusz,
   - są wyznaczone role i osoby odpowiedzialne,
   - posiadasz alternatywne ścieżki (backup systemów, zastępczy dostawcy, praca zdalna itp.),
   - potrafisz przywrócić działanie w czasie akceptowalnym dla biznesu (RTO).
4. Udokumentuj wnioski, zaktualizuj procedury i zaplanuj regularne testy (np. raz w roku).

Cel na lipiec: po takim ćwiczeniu nikt w organizacji nie powinien mieć wątpliwości, kto, co i w jakiej kolejności robi, gdy „gasimy pożar".

Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

Norma ISO 22301 pomaga organizacjom planować reakcję na zakłócenia, ale nie wymaga formalnej analizy wpływu na biznes (BIA) – sposób oceny można dobrać całkowicie dowolnie.

PRAWDA ☐ **FAŁSZ** ☐

ISO 22301 może być stosowana w każdej organizacji – niezależnie od branży, wielkości czy sektora – bo koncentruje się na procesach krytycznych i ciągłości, a nie na konkretnej technologii.

PRAWDA ☐ **FAŁSZ** ☐

Jednym z kluczowych wymogów ISO 22301 jest ustanowienie, wdrożenie, utrzymywanie i doskonalenie systemu zarządzania ciągłością działania (BCMS), opartego m.in. na analizie ryzyka i Business Impact Analysis.

PRAWDA ☐ **FAŁSZ** ☐

1 odpowiedź - fałsz. 2 odpowiedź - prawda. 3 odpowiedź -prawda

Quantifier.ai

SIERPIEŃ

Miesiąc zarządzania dostawcami

Skuteczne zarządzanie dostawcami to tarcza, która chroni organizację przed ryzykiem, lukami w bezpieczeństwie i niezgodnością w całym łańcuchu dostaw.

Miesiąc zarządzania łańcuchem dostaw

To system zasad, procesów, narzędzi i mechanizmów kontrolnych, które pozwalają organizacji zarządzać ryzykami, jakością, bezpieczeństwem, zgodnością regulacyjną i odpowiedzialnością w całym łańcuchu dostaw.

Obejmuje to m.in.:

- identyfikację i klasyfikację dostawców,
- ocenę ryzyk związanych z usługami i produktami,
- wymagania dotyczące bezpieczeństwa informacji i ciągłości działania,
- obowiązki ESG i etyczne,
- monitorowanie zgodności i jakości usług,
- procesy wdrożenia, offboardingu i zatwierdzania dostawców,
- zarządzanie incydentami i raportowaniem, także gdy dotyczą one stron trzecich.

Dobrze zorganizowany proces pozwala firmie uniknąć luk w bezpieczeństwie, ryzyk operacyjnych, kar regulacyjnych oraz wizerunkowych skutków naruszeń po stronie dostawców.

Kluczowe statystyki

35,5%

wszystkich naruszeń danych w 2024 r. wynikało z kompromitacji podmiotów trzecich, co pokazuje, że słaby dostawca jest dziś jednym z głównych wektorów ataku.*

98%

organizacji ma relację z co najmniej jednym dostawcą, który w ostatnich dwóch latach doświadczył naruszenia bezpieczeństwa, więc „u nas problemu nie ma” jest po prostu iluzją.**

Quantifier.ai

* https://www.darkreading.com/cyberattacks-data-breaches/securityscorecard-2025-report-surge-vendor-driven-attacks
** https://iglutech.com/2025/01/take-charge-mastering-third-party-risk-management

Dlaczego warto dbać o relacje z dostawcami?

Silne i świadomie budowane relacje z dostawcami są kluczowym elementem stabilności operacyjnej, bezpieczeństwa informacji, zarządzania ryzykiem oraz odpowiedzialnego łańcucha dostaw. Dobre partnerstwo biznesowe wpływa nie tylko na jakość usług i produktów, ale także na wiarygodność organizacji oraz jej odporność na zakłócenia.

- **Niższe ryzyko operacyjne i biznesowe**

Dostawcy z wysokim poziomem zaangażowania i komunikacji są bardziej skłonni reagować proaktywnie na problemy, informować o zagrożeniach oraz wspierać w sytuacjach kryzysowych.

- **Lepsza jakość usług i ciągłość działania**

Dobre relacje przekładają się na wyższą jakość realizacji umów, terminowość, większą elastyczność oraz większą gotowość do wprowadzania usprawnień.

- **Zgodność z regulacjami**

Coraz więcej przepisów nakłada na organizacje obowiązek nadzorowania dostawców. Regularna współpraca ułatwia gromadzenie danych, weryfikację zgodności i realizację due diligence.

- **Redukcja kosztów i wyższa efektywność**

Długofalowa współpraca umożliwia optymalizację procesów, standaryzację usług oraz negocjacje korzystniejszych warunków.

Formy angażowania dostawców

1. Transparentna komunikacja i regularna współpraca operacyjna
Budowanie relacji opartych na otwartości, stałym przepływie informacji i wspólnym rozwiązywaniu problemów. Obejmuje to cykliczne spotkania, przeglądy jakości usług, oczekiwań oraz aktualizację wymagań bezpieczeństwa, ESG i compliance.

2. Wspólne podnoszenie standardów i kompetencji
Zaangażowanie dostawców w szkolenia, wymianę wiedzy, udostępnianie wytycznych oraz materiałów edukacyjnych. Celem jest wyrównanie poziomu dojrzałości, budowanie kultury bezpieczeństwa oraz wspieranie dostawców w spełnianiu wymogów regulacyjnych i certyfikacyjnych.

3. Monitorowanie, ocena i rozwój partnerstwa
Ciągłe due diligence, audyty, przeglądy ryzyk, ocena SLA/KPI oraz planowanie działań rozwojowych. Zamiast jednorazowych kontroli tworzenie długofalowego partnerstwa opartego na ciągłym monitoringu, feedbacku i wspólnym doskonaleniu procesów.

Lista kontrolna: 9 pytań do dostawców

1. Jakie usługi lub produkty dostawca świadczy i jak krytyczne są one dla naszej działalności?
2. Czy dostawca posiada ważne certyfikacje z zakresu bezpieczeństwa i zgodności (np. ISO 27001, SOC 2, gotowość NIS2)?
3. Do jakich danych dostawca będzie miał dostęp, jakie będzie przetwarzał lub przechowywał w naszym imieniu?
4. Jakie środki bezpieczeństwa stosuje dostawca w celu ochrony naszych danych i usług?
5. Jak wygląda proces reagowania na incydenty po stronie dostawcy i jak szybko musi nas o nich powiadomić?
6. Jakie podmioty trzecie i podwykonawcy są wykorzystywani przez dostawcę? Czy korzystają z dalszych procesorów lub zewnętrznych usługodawców?
7. Jakie ryzyka finansowe, operacyjne lub geopolityczne mogą wpływać na niezawodność dostawcy?
8. Jakie są możliwości dostawcy w zakresie ciągłości działania i odtwarzania po awarii?
9. Jakie są możliwości dostawcy w zakresie ciągłości działania i odtwarzania po awarii?

Najważniejsze regulacje dotyczące dostawców

NIS2 – Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej

- Wymaga oceny ryzyk dostawców, stosowania wymogów bezpieczeństwa wobec podmiotów trzecich, nadzoru nad łańcuchem dostaw oraz zgłaszania incydentów, również tych po stronie dostawców.

ISO/IEC 27001 – Międzynarodowa norma zarządzania bezpieczeństwem informacji

- Nakłada obowiązek posiadania procedury zarządzania dostawcami, oceny ich ryzyk, określania wymagań bezpieczeństwa w umowach oraz ciągłego monitorowania zgodności.

CSRD – Corporate Sustainability Reporting Directive (Dyrektywa o raportowaniu zrównoważonego rozwoju)

- Zobowiązuje do raportowania wpływów środowiskowych i społecznych w całym łańcuchu wartości, uwzględnia emisje Scope 3 oraz wymaga ESG due diligence dostawców.

CSDDD – Corporate Sustainability Due Diligence Directive (Dyrektywa o należytej staranności w łańcuchu dostaw)

- Wprowadza obowiązkowe due diligence w łańcuchu dostaw: monitorowanie ryzyk, przeciwdziałanie naruszeniom praw człowieka i środowiska oraz wdrażanie działań naprawczych wobec dostawców.

EUDR – EU Deforestation Regulation (Rozporządzenie UE dotyczące zapobiegania wylesianiu)

- Wymaga pełnej identyfikowalności surowców, geolokalizacji oraz potwierdzenia ich legalnego i niewylesiającego pochodzenia.

RODO/GDPR – Rozporządzenie o Ochronie Danych Osobowych

- Dostawca przetwarzający dane osobowe musi działać zgodnie z RODO, mieć umowę powierzenia (DPA), a incydenty po jego stronie są równocześnie incydentami administratora danych.

1 SIERPNIA

DZIEŃ WORLD WIDE WEB

Ten wyjątkowy dzień upamiętnia narodziny sieci WWW i przypomina o transformacyjnym wpływie, jaki wywarła ona na nasze życie. To okazja, by docenić niesamowitą moc internetu w łączeniu ludzi, idei i informacji na całym świecie. Tak jak WWW zrewolucjonizował sposób, w jaki przepływają informacje, tak dziś organizacje muszą postrzegać swoich dostawców jako integralne elementy jednego, współzależnego ekosystemu.

ROZPOZNAJ RED FLAGĘ DOSTAWCY

🚩 Red flag:	Skutek:
Dostawca odmawia podpisania umowy powierzenia danych (DPA), twierdząc, że „nie jest potrzebna”.	Brak gotowości do zgodności z RODO = poważne ryzyko prawne i operacyjne.
Dostawca twierdzi, że ma ISO 27001, ale nie chce pokazać certyfikatu ani zakresu certyfikacji.	Brak dowodu = brak zaufania. Certyfikat bez potwierdzenia nie istnieje.
Dostawca nie ma ustalonego SLA ani procedury obsługi incydentów.	W przypadku incydentu nikt nie wie, kto odpowiada i w jakim czasie.
Dostawca korzysta z podwykonawców, ale nie chce ujawnić, kto nimi jest.	Brak transparentności = ryzyka 4. poziomu.
Dostawca twierdzi, że „nigdy nie miał incydentu”.	Firmy bez incydentów nie istnieją — istnieją tylko te, które ich nie zauważają.
Dostawca prosi o pełen dostęp administratora, choć technicznie nie jest mu potrzebny.	Over-permissioning = katastrofa do odhaczenia.
Dostawca nie ma polityki bezpieczeństwa ani dokumentacji procesów.	Brak podstaw to brak kontroli nad całym systemem.
Dostawca nie chce uczestniczyć w przeglądach dostawców ani audycie.	Dobry dostawca to partner — nie uciekinier.

WRZESIEŃ

Miesiąc norm ISO

Dbajmy o międzynarodowe standardy określające wymagania wobec systemów zarządzania

Miesiąc normy ISO

Normy ISO to międzynarodowe standardy określające wymagania wobec systemów zarządzania różnymi obszarami działalności. Przykładowo, ISO 9001 definiuje system zarządzania jakością (skupiający się na spełnianiu wymagań klienta i ciągłym doskonaleniu), ISO 14001 dotyczy zarządzania środowiskowego, ISO/IEC 27001 bezpieczeństwa informacji, a ISO 50001 – zarządzania energią. Dzięki wspólnej strukturze (tzw. „high-level structure") normy te są łatwiejsze do zintegrowania między sobą, co przekłada się na efektywność procesów i jednoznaczną komunikację wymagań w organizacji.. Implementacja norm ISO zwiększa efektywność wykorzystania zasobów, ułatwia zarządzanie ryzykiem i wzmacnia zaufanie interesariuszy.

W obszarze compliance kluczowa jest rola audytów: audyt wewnętrzny (przeprowadzany przez pracowników lub współpracowników organizacji) oraz audyt zewnętrzny (certyfikujący realizowany przez niezależne jednostki) weryfikują zgodność procesów z normami. ISO 19011 – międzynarodowy standard dla audytorów - definiuje zasady i dobrą praktykę prowadzenia audytów systemów zarządzania, akcentując zarządzanie programem audytów oraz podejście oparte na ryzyku. Audyty pozwalają wykryć luki w systemie, wypracować działania korygujące i utrwalać kulturę ciągłej poprawy w duchu compliance.

Kluczowe statystyki

80,

to liczba międzynarodowych norm ISO dotyczących systemów zarządzania (MSS) funkcjonujących obecnie na świecie.*

24 000,

to przybliżona liczba wszystkich opublikowanych norm ISO obejmujących różne dziedziny gospodarki.**

300 410,

to liczba certyfikatów ISO 14001 (system zarządzania środowiskowego) w 2023 roku.***

Quantifier.ai

* https://amtivo.com/ie/resources/insights/iso-certification-journey-ultimate-faq-guide/
** https://www.iso.org/news/From-aspirations-to-action.html
*** https://www.studocu.com/es/document/universidad-rey-juan-carlos/direccion-estrategica-y-politica-de-empresa-ii/casco-2024-iso-survey-of-management-system-certifications-2023/130069192

Case study: TechPro Sp. z o. o

Przykładowa firma produkcyjna „TechPro Sp. z o.o." zdecydowała się na certyfikację ISO 9001 (system zarządzania jakością). W ramach wdrożenia przeprowadzono analizę procesów produkcyjnych i określono kluczowe wskaźniki jakości. Podczas audytu wewnętrznego zidentyfikowano powtarzający się defekt w jednej z linii produkcyjnych.

Dzięki temu firma wprowadziła korekty procedur, przeszkolono pracowników i zaostrzyła nadzór - co przyniosło znaczące zmniejszenie reklamacji klientów. W kolejnym audycie zewnętrznym (certyfikującym) potwierdzono spełnienie wymagań ISO 9001 oraz otrzymano rekomendację ulepszeń dokumentacji. Przykład „TechPro" pokazuje, że audyt (wewnętrzny i zewnętrzny) nie tylko weryfikuje zgodność, ale i inicjuje realne usprawnienia, przekładające się na lepsze wyniki biznesowe i zaufanie klientów.

Czy wiesz że....

Wśród pozostałych popularnych norm wymienia się m.in. ISO 45001 (system zarządzania bezpieczeństwem pracy – ok. 185 000 certyfikatów) oraz ISO 37001 (przeciwdziałanie korupcji). Wiele firm wdraża jednocześnie kilka norm (tzw. zintegrowany system zarządzania), co ułatwia wspólna struktura standardów ISO.

Audyt wewnętrzny ma niebagatelny wpływ na wyniki firmy – wdrażając ISO 19011, organizacje usprawniają program audytów, a z wytycznych ISO wynika, że sprawdzanie zgodności z procedurami pozwala systematycznie ograniczać niezgodności i marnotrawstwo (tzw. cykl PDCA: plan – do – check – act).

Wyzwanie na wrzesień

Przeprowadź wewnętrzny audyt próbny jednego procesu: Wybierz dowolny obszar (np. produkcję, HR, ochronę środowiska) i sprawdź, czy procedury realizowane są zgodnie z wybraną normą ISO. Przeprowadź audyt wewnętrzny (lub checklistę kontrolną), przygotuj sprawozdanie z niezgodności i zaplanuj działania korygujące. Ten praktyczny krok pozwoli zweryfikować gotowość organizacji do ewentualnej certyfikacji i wzmocnić kulturę ciągłej poprawy w duchu zgodności.

Lista kontrolna - normy ISO

1. **Zdefiniowane cele i procedury:**
Czy kluczowe procesy (np. produkcja, HR, IT) są udokumentowane, a cele jakościowe/środowiskowe/sieciowe określone?

2. **Przeprowadzone audyty wewnętrzne:**
Czy istnieje plan audytów wewnętrznych (zgodnie z ISO 19011)? Czy ostatnie audyty wykazały ewentualne niezgodności i wdrożono działania korygujące?

3. **Szkolenia pracowników:**
Czy personel rozumie znaczenie norm ISO i posiada przeszkolenie z zakresu swoich obowiązków w systemie zarządzania?

4. **Zarządzanie ryzykiem:**
Czy organizacja ma proces oceny i przeglądu ryzyk związanych z jakością, bezpieczeństwem czy środowiskiem?

5. **Certyfikaty i audyty zewnętrzne:**
Czy firma planuje lub posiada certyfikację zewnętrzną ISO? Czy uwzględniono wymogi audytorów zewnętrznych (np. dostęp do dokumentacji, rejestry)?

6. **Kultura zgodności:**
Czy w organizacji promuje się postawy proaktywne – zgłaszanie błędów i sugestii usprawnień (analogia do mechanizmów whistleblowingu) oraz konsekwentne przestrzeganie ustalonych procedur?

26 WRZEŚNIA

DZIEŃ DUMY AUDYTORA

Coroczne święto obchodzone w ostatni czwartek września, mające na celu uhonorowanie wkładu i znaczenia zawodu audytora, podkreślenie jego roli w zapewnianiu rzetelności, transparentności i stabilności finansowej w biznesie.

Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

	PRAWDA	FAŁSZ
Certyfikacja ISO jest obowiązkowa – każda firma musi uzyskać certyfikat, żeby działać zgodnie z przepisami.	☐	☐
Wiele norm ISO (np. ISO 9001, 14001, 50001) korzysta ze wspólnej struktury i pojęć (Annex SL), co ułatwia integrowanie wymagań w ramach jednego systemu zarządzania.	☐	☐
ISO 9001 koncentruje się na zadowoleniu klienta i ciągłym doskonaleniu procesów – firmy certyfikowane wg tej normy muszą mierzyć i poprawiać swoją jakość oraz reagować na opinie klientów.	☐	☐

1 odpowiedź - fałsz. 2 odpowiedź -prawda. 3 odpowiedź - prawda

Quantifier.ai

PAŹDZIERNIK

Miesiąc ESG

Październik to miesiąc poświęcony tematyce ESG (środowisko, społeczeństwo, ład korporacyjny)

Miesiąc ESG

Zarządzanie ESG stało się jednym z kluczowych elementów strategii przedsiębiorstw, głównie ze względu na rosnące wymogi regulacyjne w Unii Europejskiej. Firmy muszą uwzględniać kwestie środowiskowe, społeczne i ładu korporacyjnego w raportowaniu oraz due diligence, a brak dostosowania oznacza realne ryzyko prawne, finansowe i reputacyjne.

- CSRD – dyrektywa o sprawozdawczości zrównoważonego rozwoju (2022/2464), rozszerza NFRD i obejmie ok. 6 tys. dużych firm w UE oraz ok. 900 dużych firm spoza UE.
- ESRS – europejskie standardy raportowania opracowane przez EFRAG na potrzeby CSRD; definiują strukturę i zakres ujawnień ESG.
- SFDR – rozporządzenie 2019/2088 zobowiązujące instytucje finansowe do ujawniania, jak uwzględniają ryzyka i skutki zrównoważonego rozwoju w swoich produktach i decyzjach inwestycyjnych.
- Taksonomia UE – regulacja 2020/852, system klasyfikacji „zielonych" działalności gospodarczych zgodnych z celami klimatycznymi i środowiskowymi.
- CSDDD – dyrektywa 2024/1760 wprowadzająca obowiązek należytej staranności (due diligence) w łańcuchach dostaw w obszarze praw człowieka i środowiska oraz wymóg planów przejścia na gospodarkę neutralną klimatycznie.
- Wniosek dla firm – rosnąca gęstość regulacji sprawia, że przygotowanie organizacji do ESG compliance staje się elementem zarządzania ryzykiem i warunkiem utrzymania konkurencyjności.

Kluczowe statystyki

500 000 000 USD

rocznych globalnych przychodów to próg, powyżej którego firmy prowadzące działalność w Kalifornii podlegają obowiązkowi cyklicznego raportowania klimatycznych ryzyk finansowych na mocy SB 261, choć egzekwowanie tej ustawy jest obecnie tymczasowo wstrzymane przez sąd.*

2 600 / 4 100

2 600 spółek ma wstępnie podlegać obowiązkowi raportowania emisji GHG na mocy SB 253, a około 4 100 spółek ma być objętych SB 261 w zakresie raportowania klimatycznego ryzyka finansowego, według wstępnej listy opublikowanej przez CARB.**

Quantifier.ai

* https://ww2.arb.ca.gov/our-work/programs/california-corporate-greenhouse-gas-ghg-reporting-and-climate-related-financial

** https://corpgov.law.harvard.edu/2025/10/12/carb-publishes-preliminary-list-of-companies-potentially-subject-to-sb-253-and-sb-261

Case study: Producent leków

Wyobraźmy sobie spółkę „GreenGrow S.A." – producenta leków działającego na rynkach UE. Po wejściu w życie CSRD zarząd „GreenGrow" postanowił kompleksowo przygotować firmę. Najpierw firma przeprowadziła analizę podwójnej istotności (double materiality): zidentyfikowała kluczowe tematy ESG (emisje gazów cieplarnianych, etyczne źródła surowców, zdrowie i bezpieczeństwo pracowników). Następnie opracowano strategię redukcji śladu węglowego (celem jest zgodność z porozumieniem paryskim) i wdrożono mechanizmy monitorowania danych (system pomiaru emisji, raportowanie w systemie ESEF). Dla potrzeb łańcucha dostaw „GreenGrow" przygotował mapy ryzyk w łańcuchu dostaw – np. sprawdzono, czy dostawcy substancji czynnych przestrzegają praw pracowniczych. W efekcie, gdy urzędnik państwowy lub audytor poprosił o dokumentację ESG, firma była w stanie przedstawić kompletną sprawozdawczość zgodnie z ESRS i aktywny plan due diligence. Gdyby „GreenGrow" nie wdrożył tych kroków, mogłaby zostać narażona na sankcje (np. kary finansowe w ramach prawa krajowego), a także stracić zaufanie inwestorów odpowiedzialnych (ESG), co w dłuższej perspektywie groziło by np. ograniczeniem dostępu do kapitału.

Czy wiesz że....

Skala CSRD:
Nowa dyrektywa obejmie dziesiątki tysięcy firm w UE, w tym ok. 6 tys. dużych spółek z UE i ~900 spoza UE. Poprzednia NFRD dotyczyła jedynie ok. 11 tys. firm.

Obowiązki w finansach (SFDR):
Instytucje finansowe muszą ujawniać, jak uwzględniają ryzyka zrównoważonego rozwoju i wpływ swoich inwestycji. Regulacja nie wymusza inwestowania wyłącznie w zielone aktywa, ale wymaga uzasadniania deklaracji ESG.

Taksonomia UE:
Wspólna klasyfikacja działalności zrównoważonej z technicznymi kryteriami dla celów klimatycznych i środowiskowych. Ułatwia zrozumienie, co faktycznie kwalifikuje się jako „zielone".

Globalne trendy:
Chiny wprowadzają obowiązkowe raportowanie ESG od 2026. Szwajcaria wymaga ujawniania ryzyk klimatycznych według TCFD od 2024. W USA regulacje federalne stoją w miejscu, ale Kalifornia wprowadza obowiązkowe raportowanie emisji dla firm powyżej 1 mld USD od 2026 i ryzyk klimatycznych od 500 mln USD przychodu.

Lista kontrolna - ESG

1. **Identyfikacja regulacji:** Upewnij się, które przepisy ESG dotyczą twojej organizacji (CSRD, SFDR, taksonomia UE, itp.). Kalendarz obowiązków: od kiedy zaczynają się nowe terminy sprawozdawcze?

2. **System raportowania:** Czy firma ma procesy zbierania i weryfikacji danych ESG (emisje, zużycie energii, społeczna odpowiedzialność, struktura zarządzania itp.)? Czy są one zgodne z wymaganiami ESRS i SFDR?

3. **Analiza podwójnej istotności:** Czy przeprowadzono ocenę wpływu firmy na otoczenie (inside-out) oraz wpływu czynników zewnętrznych na działalność firmy (outside-in)? Jakie tematy ESG uznano za najważniejsze?

4. **Strategia ESG i plany działania:** Czy istnieje dokument wdrażający cele środowiskowe (np. plan redukcji emisji), społeczne i zarządcze? Czy uwzględniono cele klimatyczne zgodne z Porozumieniem Paryskim?

5. **Due diligence w łańcuchu dostaw:** Czy firma zmapowała i oceniła ryzyka praw człowieka i środowiskowe u swoich dostawców? Czy wdrożono procedury zapobiegania naruszeniom (audyt dostawców, zapisy w umowach)?

6. **Wewnętrzny audyt i szkolenia:** Czy przeprowadzono wstępny audyt (gaps analysis) pod kątem ESG i przygotowano pracowników (szkolenia w zakresie nowych procedur)?

7. **Konsekwencje niezgodności:** Czy firma zdaje sobie sprawę z kar i ryzyk wynikających z niedostosowania (np. kary finansowe, ryzyko wykluczenia z zamówień publicznych, utrata inwestorów)?

24 PAŹDZIERNIKA

MIĘDZYNARODOWY DZIEŃ ONZ

Z okazji Dnia ONZ - święta promującego idee pokojowego i zrównoważonego rozwoju. W kontekście compliance kluczowe jest zrozumienie rosnącego znaczenia regulacji ESG w prawie polskim i międzynarodowym. Firmy muszą dostosować się do nowych obowiązków raportowania zrównoważonego rozwoju, aby sprostać oczekiwaniom inwestorów, regulatorów i społeczeństwa.

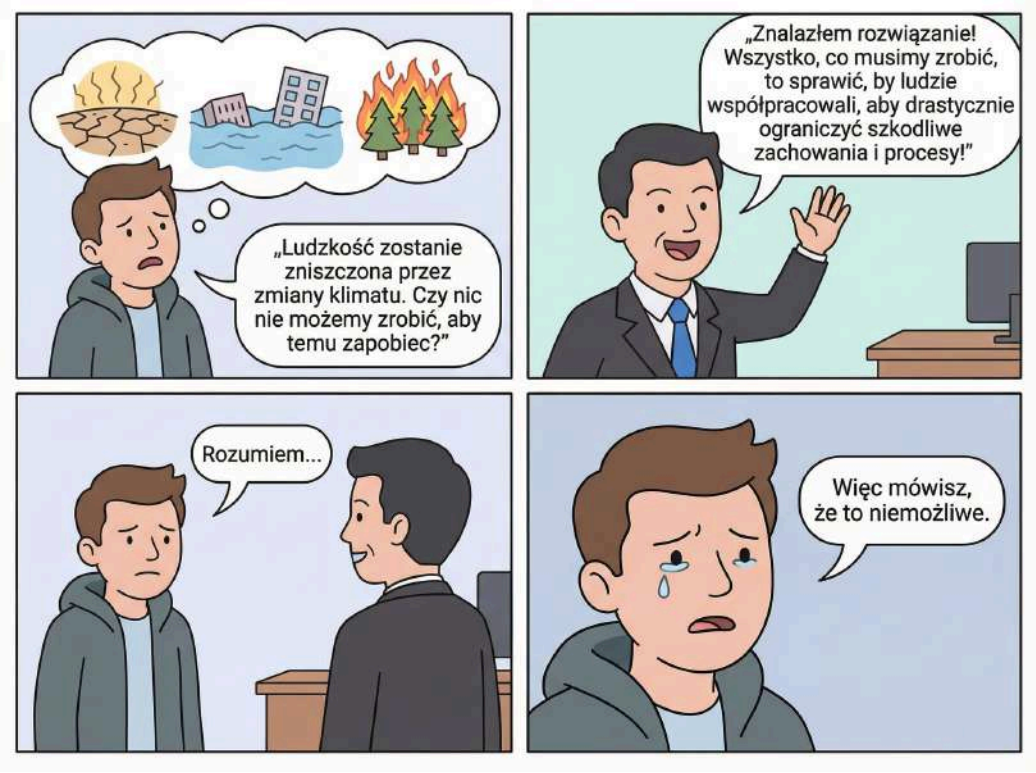
Wyzwanie na październik

Zadanie praktyczne: Sprawdź swoją mini checklistę ESG:

E - Środowisko (Environmental)
□ Czy organizacja mierzy i raportuje emisje CO_2 (zakres 1 i 2, a docelowo 3)?
□ Czy mamy cele klimatyczne zgodne z Porozumieniem Paryskim?
□ Czy posiadamy politykę środowiskową (gospodarka odpadami, energia, woda)?
□ Czy uwzględniamy zasady gospodarki obiegu zamkniętego (GOZ) w produktach/usługach?

S – Społeczeństwo (Social)
□ Czy zapewniamy bezpieczne i równe warunki pracy?
□ Czy monitorujemy zgodność łańcucha dostaw z prawami człowieka (due diligence)?
□ Czy mamy politykę różnorodności, równości i inkluzywności (DEI)?
□ Czy organizacja angażuje się w inicjatywy społeczne lub edukacyjne?

G – Ład korporacyjny (Governance)
□ Czy zarząd nadzoruje kwestie ESG i podejmuje decyzje w oparciu o ryzyka niefinansowe/ESG?
□ Czy mamy politykę antykorupcyjną i kanał zgłaszania nieprawidłowości (whistleblowing)?
□ Czy publikujemy dane ESG zgodnie z obowiązującymi regulacjami (np. CSRD/ESRS)?
□ Czy wynagrodzenia kadry zarządzającej są powiązane z celami ESG?



Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

Dyrektywa CSRD wymaga, by przedsiębiorstwa określiły cele klimatyczne i przedstawiły plan ich realizacji (zgodne z Porozumieniem Paryskim) w swoich strategiach lub ujawniły, że ich nie mają.

PRAWDA ☐ **FAŁSZ** ☐

Unijny SFDR nakłada na zarządzających aktywami obowiązek ujawniania proporcji inwestycji zgodnych z taksonomią UE oraz wyjaśniania, w jaki sposób ryzyka ESG wpływają na wyniki funduszy.

PRAWDA ☐ **FAŁSZ** ☐

Na mocy nowych regulacji wszystkie spółki muszą od razu raportować ESG w pełnym standardzie CSRD – nawet małe prywatne firmy.

PRAWDA ☐ **FAŁSZ** ☐

1 odpowiedź - prawda. 2 odpowiedź prawda. 3 odpowiedź - fałsz

Quantifier.ai

LISTOPAD

Miesiąc AI Act

Listopad poświęcamy regulacjom prawnym dotyczącym sztucznej inteligencji.

Miesiąc AI i Prawa

W 2024 r. Unia Europejska przyjęła Rozporządzenie o sztucznej inteligencji („AI Act"), pierwszą na świecie prawodawczą próbę klasyfikacji i regulacji systemów AI według poziomu ryzyka. AI Act przewiduje cztery poziomy ryzyka: niedopuszczalne (zakazane praktyki, np. systemy oceny wiarygodności społecznej prowadzone przez państwo), wysokie (obowiązkowe surowe wymogi dla AI mających znaczący wpływ na zdrowie, bezpieczeństwo lub prawa człowieka), ograniczone (ograniczone obowiązki transparentności, np. chatboty muszą poinformować, że to AI) oraz minimalne (brak dodatkowych wymogów). Systemy wysokiego ryzyka (np. AI w diagnostyce medycznej, rekrutacji, zarządzaniu infrastrukturą) będą podlegać obowiązkowi prowadzenia zarządzania ryzykiem, testom i dokumentacji (m.in. ocena bezpieczeństwa, ochrona danych, dokumentowane techniki).

Równolegle ISO opracowało ISO/IEC 42001 – pierwszy standard zarządzania AI. Definiuje on ramy systemu zarządzania sztuczną inteligencją, analogicznie do ISO 9001 czy 27001, umożliwiając organizacjom systematyczne podejście do ryzyk i możliwości AI. Zawiera wytyczne dotyczące procesów ryzyka, kontroli i cyklu życia systemów AI. W świetle AI Act i ISO 42001 firmy korzystające z AI powinny zadbać o dokumentację (oceny ryzyka, polityki użytkowania AI, audyty algorytmiczne itp.), wdrożenie systemu zarządzania oraz odpowiedzialny nadzór. Compliance musi więc teraz objąć również aspekty technologiczne: prawnicy i specjaliści ds. zgodności powinni współpracować z działami IT i R&D, by sprostać oczekiwaniom regulacyjnym dotyczącym AI.

Kluczowe statystyki

35 MLN EURO

lub 7% światowego rocznego obrotu przedsiębiorstwa (zależnie od tego, która wartość jest wyższa) to maksymalna kara administracyjna przewidziana przez AI Act za najpoważniejsze naruszenia, takie jak używanie zakazanych systemów AI, co stawia te sankcje na poziomie porównywalnym lub wyższym niż RODO.*

5 MLD EURO

rocznie oszczędności w kosztach administracyjnych do 2029 r. szacuje Komisja Europejska dzięki pakietowi zmian określanemu jako „digital omnibus", który obejmuje m.in. odroczenie części obowiązków z AI Act i uproszczenie wybranych wymogów cyfrowych.**

* https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-99
** https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718

Case study: Dostawca usług finandsowych

Załóżmy, że firma „FinBot Solutions" – dostawca usług finansowych – wdraża nowy system AI do analizy zdolności kredytowej klientów. Ten system może wpływać na życie klienta, więc w EU będzie uznany za wysokiego ryzyka. W przygotowaniu do wdrożenia „FinBot" przeprowadza ocenę ryzyka: dokumentuje sposób działania algorytmu, dane treningowe, scenariusze ewentualnego niewłaściwego działania. Dział compliance współpracuje z IT nad uzupełnieniem procesów: tworzy obowiązkowy rejestr systemów AI, plan reagowania na incydenty (w razie błędów algorytmu), zapewnia przestrzeganie ochrony danych osobowych (wskaźniki DPIA) i prowadzi audyt wewnętrzny. Dzięki temu, gdy regulator zażąda dokumentów (raportu o ryzyku, wyników testów, dowodów szkolenia personelu), firma jest przygotowana. Dodatkowo „FinBot" wprowadza szkolenia dla pracowników i instrukcje użytkowania AI. Gdyby firma pominęła te kroki, mogłaby narazić się na sankcje (kara za wprowadzenie na rynek niebezpiecznego systemu) oraz poważne ryzyko reputacyjne (awaria algorytmu lub skarga klienta).

Czy wiesz że....

- Nowe prawo UE: Parlament Europejski ostatecznie zatwierdził AI Act w maju 2024 – będzie on stopniowo wchodził w życie (większość wymogów dla wysokiego ryzyka zacznie obowiązywać po ~2 latach od publikacji rozporządzenia). Obejmuje on między innymi obowiązek ciągłego zarządzania ryzykiem w systemach AI oraz wymóg dokumentowania danych i testów.

- Standard zarządzania AI: ISO/IEC 42001 został opublikowany w grudniu 2023 i stanowi pierwszy na świecie standard dotyczący systemu zarządzania AI.. Normy powiązane (ISO 42002, 42003 itp.) są w trakcie opracowywania, skupiają się m.in. na jakości danych i interoperacyjności AI.

- Ryzyka komunikacyjne: Generatywne modele językowe (chatboty, narzędzia do tłumaczeń, analizy treści) tworzą nową kategorię „komunikacji AI", co znacząco komplikuje procesy nadzoru i archiwizacji firmowej (tzw. aiComms). Oznacza to, że dotychczasowe rozwiązania compliance często nie radzą sobie z kontrolą tak dużej ilości treści generowanej automatycznie. W praktyce konieczne jest korzystanie z nowych narzędzi do monitoringu i archiwizacji AI.

Lista kontrolna - AI

1. **Inwentaryzacja systemów AI:** Spisz wszystkie zastosowania AI w organizacji (systemy eksperckie, chatboty, analizy danych, automatyczne decyzje itp.). Określ, czy którykolwiek spełnia kryteria wysokiego ryzyka według AI Act (np. używany w rekrutacji, diagnostyce, sądach).

2. **Ocena ryzyka i dokumentacja:** Dla każdego identyfikowanego systemu AI przygotuj ocenę ryzyka (np. zgodnie z ISO 31000 + specyficzne ryzyka AI). Zarejestruj wyniki w dokumentacji: analiza danych treningowych, potencjalne negatywne skutki, środki zaradcze. W przypadku systemów high-risk wdroż system zarządzania ryzykiem AI zgodnie z AI Act (ciągły proces analiz i kontroli).

3. **Compliance i audyt:** Sprawdź, czy proces zakupu/rozwijania systemów AI uwzględnia wymagania compliance. Czy każdego „wysokiego ryzyka" AI weryfikuje zewnętrzna strona (certyfikacja przez notyfikowany organ)? Czy istnieją procedury audytu dla algorytmów (np. testy jakości danych)?

4. **Edukacja i polityki:** Przeszkol zespoły w zakresie nowych regulacji AI (AI Act) i dobrych praktyk (np. unikanie biasu). Opracuj wewnętrzną politykę korzystania z AI – wskazówki, jak stosować AI w zgodzie z prawem (np. zadeklaruj użycie modeli generatywnych wobec klientów).

5. **Perspektywa compliance:** Dodaj AI do corocznego przeglądu compliance: monitoruj ewentualne zmiany prawa (np. prace nad zmianami do AI Act), wprowadź proces zgłaszania incydentów związanych z AI i uwzględnij AI w procesach audytu wewnętrznego (np. audyt treści generowanych przez AI w komunikacji firmowej).

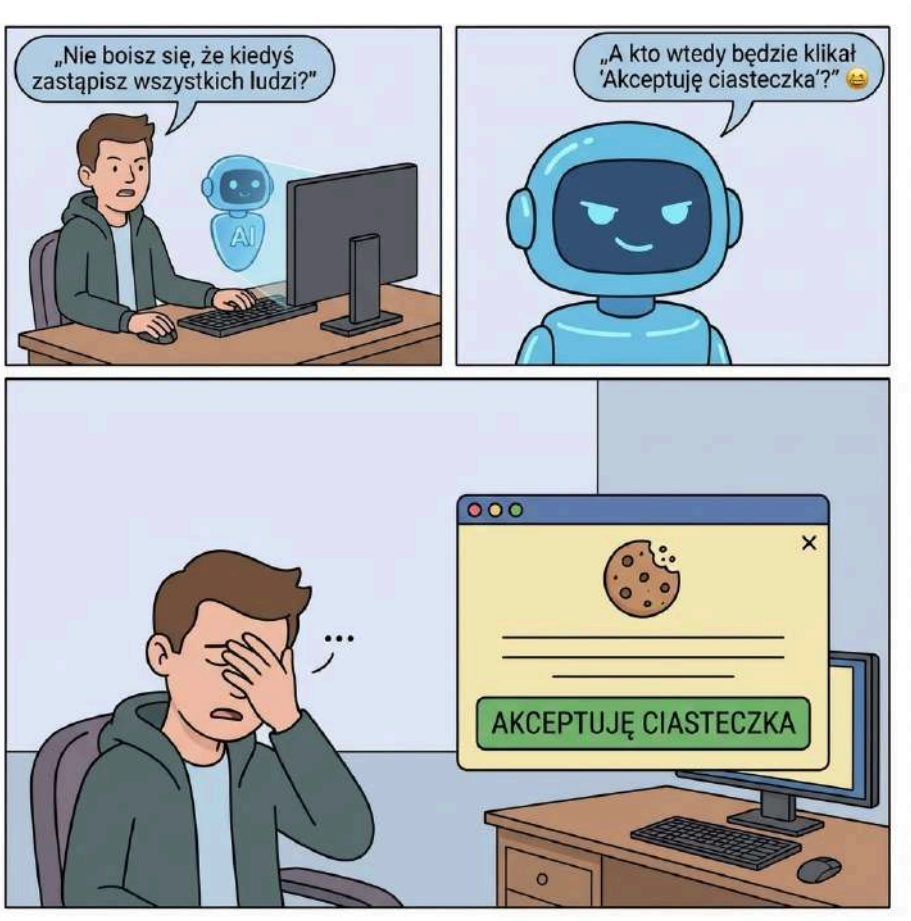
10 LISTOPADA

ŚWIATOWY DZIEŃ NAUKI DLA POKOJU I ROZWOJU

To coroczne święto, obchodzone w państwach członkowskich ONZ, zostało ustanowione przez Konferencję Generalną UNESCO w 2001 roku. Głównym celem obchodów jest m.in. podnoszenie świadomości na temat roli nauki w budowaniu pokojowego społeczeństwa.

Wyzwanie na listopad. Szybka checklista audytu zgodności narzędzia AI

1. Identyfikacja
□ Czy narzędzie jest formalnie uznane za AI?
□ Czy wiadomo, kto odpowiada za jego nadzór?
2. AI Act – zgodność
□ Czy określono kategorię ryzyka (minimalne / ograniczone / wysokie)?
□ Czy użytkownik jest poinformowany, że korzysta z AI?
3. Dane i prywatność
□ Czy wiadomo, jakie dane AI przetwarza?
□ Czy istnieje ryzyko ujawnienia danych poufnych?
□ Czy wykonano ocenę skutków (jeśli dotyczy)?
4. Ryzyka i kontrole
□ Czy zidentyfikowano potencjalne negatywne skutki działania AI?
□ Czy wdrożono podstawowe środki ograniczające (np. monitoring, akceptacja przez człowieka)?
5. Dokumentacja i nadzór
□ Czy narzędzie jest wpisane do rejestru AI w firmie?
□ Czy istnieje minimalna dokumentacja działania i ograniczeń?
□ Czy regularnie monitoruje się jakość i błędy systemu?



Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

W myśl prawa UE wszystkie systemy AI muszą być certyfikowane przez europejski organ nadzoru przed użyciem.

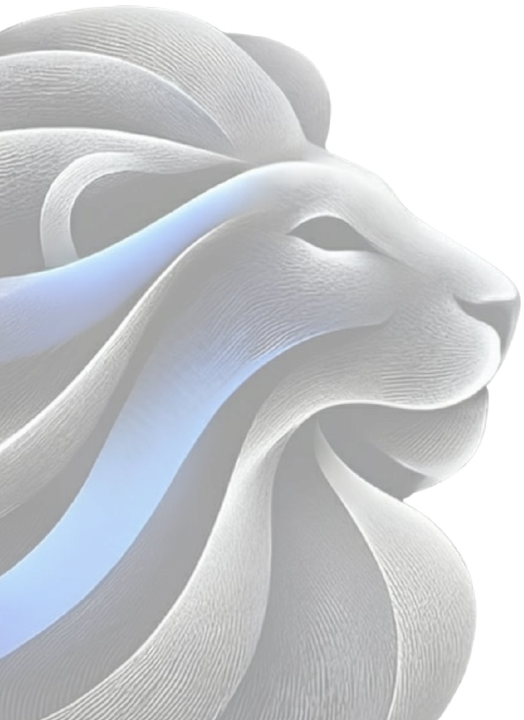
PRAWDA ☐ **FAŁSZ** ☐

Norma ISO/IEC 42001:2023 definiuje ramy systemu zarządzania sztuczną inteligencją, pomagając organizacjom wdrożyć kontrolę nad AI (podobnie jak ISO 9001 dla jakości). Warto ją wziąć pod uwagę przy budowie polityki zarządzania AI.

PRAWDA ☐ **FAŁSZ** ☐

AI Act wprowadza cztery kategorie ryzyka („niedopuszczalne", „wysokie", „ograniczone" i „minimalne"), w tym zakazuje stosowania niektórych systemów AI (np. zaawansowanej inwigilacji) oraz nakłada szczegółowe wymagania na systemy high-risk (m.in. zarządzanie ryzykiem przez cały cykl życia).

PRAWDA ☐ **FAŁSZ** ☐



1 odpowiedź -fałsz. 2 odpowiedź - prawda. 3 odpowiedź - prawda

Quantifier.ai

GRUDZIEŃ

Miesiąc KYC oraz AML

KYC i AML to nie tylko regulacje - to filtr, przez który przepuszcza się zaufanie.

Miesiąc KYC oraz AML

KYC (Know Your Customer) i AML (Anti-Money Laundering) tworzą zintegrowany system zapobiegania praniu pieniędzy oraz finansowaniu terroryzmu. Ich celem nie jest jedynie wykrywanie podejrzanych transakcji, ale przede wszystkim dogłębne poznanie klienta i zrozumienie jego profilu ryzyka.

Podstawy regulacyjne stanowią dyrektywy UE AMLD IV–VI, wytyczne FATF oraz Europejskiego Urzędu Nadzoru Bankowego (EBA), a w Polsce – Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.

Dobre praktyki KYC obejmują weryfikację tożsamości, analizę źródeł pochodzenia środków, bieżący monitoring transakcji oraz cykliczną aktualizację danych klientów. Skuteczny system AML nie opiera się na procedurach czy raportach, lecz na kulturze czujności i świadomości ryzyka w codziennej pracy.

Kluczowe statystyki

21 ,46 MLN EUR

kary nałożył 6 listopada 2025 r. bank centralny Irlandii na Coinbase Europe Limited za poważne naruszenia obowiązków AML/CFT w monitoringu transakcji: ponad 30,4 mln transakcji o wartości ponad 176 mld euro nie było właściwie monitorowanych, co pokazuje, jak bardzo zawiodły procesy KYC i bieżące due diligence.*

4,6 mld USD

W 2024 r. instytucje finansowe na całym świecie zapłaciły ponad 4,6 mld USD kar za naruszenia AML. Według Fenergo, aż 60% przypadków wykryto dopiero po audycie wewnętrznym.
Źródło: Fenergo Global Financial Crime Report 2024.**

Quantifier.ai

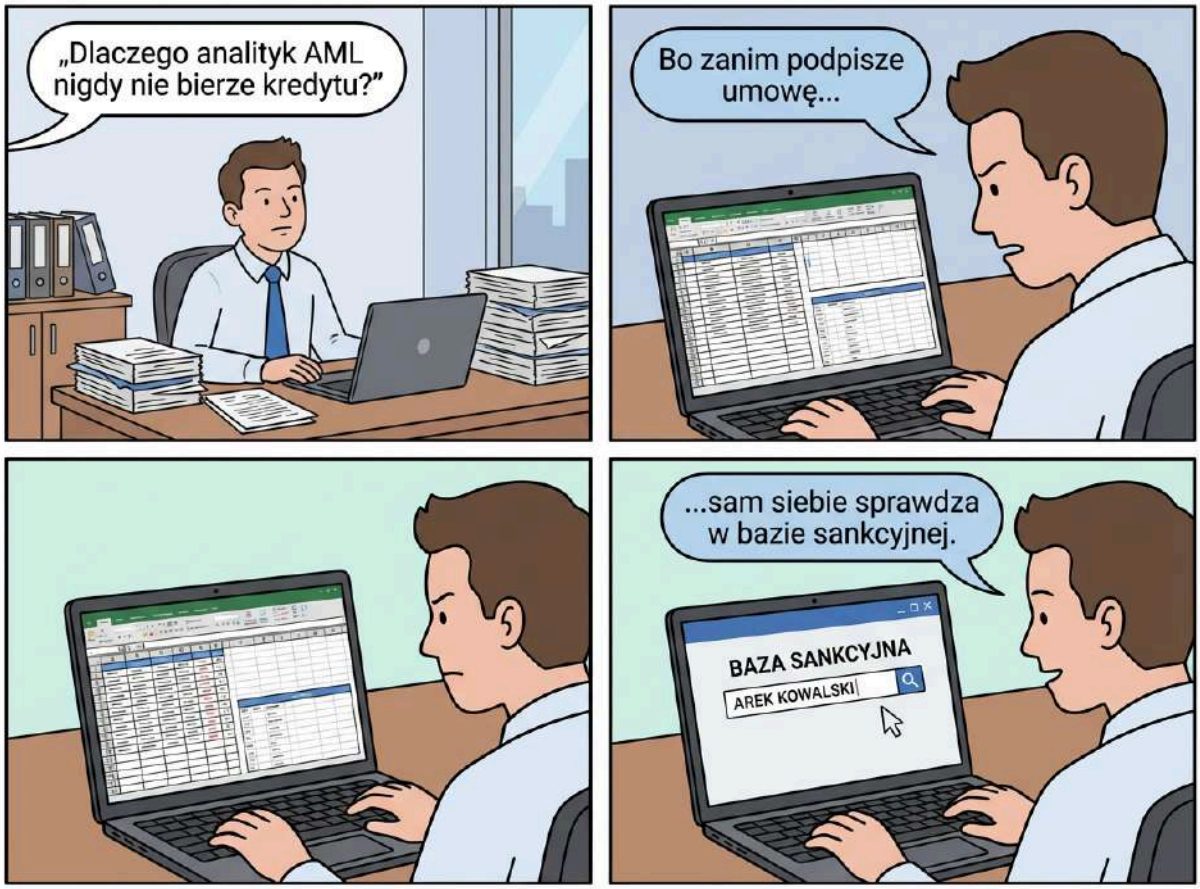
* https://www.imlovingcrypto.com/post/coinbase-europe-pod-lup%C4%85-21-5-miliona-euro-kary-od-banku-centralnego-irlandii
** https://www.corporatecomplianceinsights.com/news-roundup-january-24-2025/

Czy wiesz że....

Pierwsze zasady przeciwdziałania praniu pieniędzy (AML, anti-money laundering) pojawiły się dopiero w 1989 roku, kiedy państwa grupy G7, czyli siedmiu najbardziej uprzemysłowionych gospodarek świata, powołały do życia FATF (Financial Action Task Force). Dziś ta międzynarodowa organizacja, zrzeszająca 39 członków, wyznacza globalne standardy w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, a jej rekomendacje stanowią punkt odniesienia dla regulacji w większości krajów.

Pogromcy mitów

Mit: KYC wystarczy zrobić raz, przy onboardingu.
Fakt: Profil klienta zmienia się — tak jak jego ryzyko. Aktualizacje co 12 miesięcy to minimum, nie opcja.



Lista kontrolna - AML i KYC

1. **Ocena ryzyka i governance.** Czy organizacja ma aktualną ocenę ryzyka AML/KYC oraz zatwierdzoną strategię? Czy role i odpowiedzialności (MLRO, compliance, biznes, IT) są jasno zdefiniowane?

2. **Polityki i procedury KYC/AML.** Czy istnieją pisemne, spójne polityki i procedury KYC/AML obejmujące identyfikację klienta, beneficjentów rzeczywistych i cel relacji? Czy są regularnie aktualizowane pod kątem zmian regulacyjnych?

3. **Customer Due Diligence (CDD) i segmentacja.** Czy proces onboardingu zapewnia rzetelną weryfikację klienta i przypisanie poziomu ryzyka? Czy wymogi dokumentacyjne różnicują klientów o wyższym ryzyku?

4. **Enhanced Due Diligence (EDD).** Czy dla PEP i klientów wysokiego ryzyka stosowane są dodatkowe środki (źródło majątku, dodatkowe dokumenty, zgody wyższego szczebla)? Czy decyzje o akceptacji są formalnie udokumentowane?

5. **Monitoring transakcji i aktualizacja danych.** Czy system monitoringu odzwierciedla profil ryzyka klienta i zapewnia analizę alertów? Czy dane KYC są okresowo i zdarzeniowo aktualizowane?

6. **Screening sankcji, PEP i adverse media.** Czy prowadzony jest screening na etapie onboardingu i w trybie ciągłym? Czy istnieje jasny proces weryfikacji trafień i dokumentowania decyzji?

7. **Raportowanie, archiwizacja i testowanie systemu.** Czy procedury zgłaszania transakcji podejrzanych są stosowane w praktyce i udokumentowane? Czy archiwizacja danych i regularne testy/audyty systemu AML spełniają wymogi prawne?

4 GRUDNIA

MIĘDZYNARODOWY DZIEŃ BANKÓW

Międzynarodowy Dzień Banków obchodzony jest na całym świecie corocznie 4 grudnia , aby docenić rolę banków w dostarczaniu ludziom ważnych informacji dotyczących ich bezpieczeństwa finansowego.

Dwie prawdy i jeden fałsz.
Zaznacz prawidłową odpowiedź:

Klienci instytucjonalni nie wymagają pełnej weryfikacji KYC.

PRAWDA ☐ **FAŁSZ** ☐

Beneficjent rzeczywisty to zawsze osoba fizyczna.

PRAWDA ☐ **FAŁSZ** ☐

6AMLD wymaga penalizacji również tzw. aiding and abetting (pomocnictwa).

PRAWDA ☐ **FAŁSZ** ☐

1 odpowiedź - fałsz. 2 odpowiedź prawda. 3 odpowiedź -prawda

Quantifier.ai

DISCLAIMER

Zastrzeżenie: Niniejsze opracowanie ma charakter wyłącznie informacyjny i nie stanowi porady prawnej, podatkowej ani regulacyjnej. Zasady wynikające z przepisów (w tym m.in. RODO, NIS2, AI Act, CSRD, SFDR, regulacji AML/CFT oraz krajowych ustaw sektorowych) mogą być różnie stosowane w zależności od jurysdykcji, rodzaju podmiotu, specyfiki działalności oraz aktualnej praktyki organów nadzoru i sądów. W przypadku wątpliwości co do interpretacji lub stosowania przepisów w konkretnej sytuacji, należy skonsultować się z radcą prawnym, adwokatem, działem prawnym lub odpowiednim specjalistą (np. IOD, compliance officerem). Autorzy nie ponoszą odpowiedzialności za decyzje podjęte wyłącznie na podstawie niniejszego materiału. Warto traktować wymagania regulacyjne jako poziom minimum, a w praktyce budować rozwiązania, które wzmacniają zaufanie klientów, partnerów i organów nadzoru.

OBSERWUJ NAS

www.quantifier.ai
www.envirly.pl

www.linkedin.com/company/quantifier-ai
www.linkedin.com/company/envirly

USA: (+1) 415-799-8206
Europa: (+48) 698 759 206

contact@quantifier.ai

Quantifier.ai envirly

DZIĘKUJEMY!