					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P37					Tytuł dokumentu: **Polityka zgodności prawnej i regulacyjnej**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe ramy identyfikacji, zarządzania oraz zapewnienia zgodności ze wszystkimi obowiązkami prawnymi, regulacyjnymi i umownymi mającymi zastosowanie do bezpieczeństwa informacji, ochrony danych osobowych oraz funkcji operacyjnych organizacji.

1.2 Celem jest zapobieganie przypadkom niezgodności, które mogłyby skutkować karami finansowymi, odpowiedzialnością prawną, zakłóceniami działalności, szkodą reputacyjną lub działaniami egzekucyjnymi organów regulacyjnych.

1.3 Niniejsza polityka wspiera integrację wymagań zgodności z ładem organizacyjnym, zarządzaniem ryzykiem, procesami operacyjnymi, cyklami życia projektów oraz projektowaniem systemów.

1.4 Zapewnia ona, że wszystkie mające zastosowanie obowiązki — w różnych jurysdykcjach, sektorach branżowych i obszarach regulacyjnych — są w organizacji jednoznacznie dokumentowane, oceniane, monitorowane i egzekwowane.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich działów, funkcji, jednostek biznesowych oraz osób działających w imieniu organizacji, w tym:

2.1.1 Pracowników zatrudnionych na stałe i personelu tymczasowego

2.1.2 Wykonawców, konsultantów i stażystów

2.1.3 Zewnętrznych dostawców, podmiotów przetwarzających lub partnerów, którzy przetwarzają dane organizacji, korzystają z jej systemów lub realizują obowiązki regulacyjne

2.1.4 Każdego procesu biznesowego, projektu lub inicjatywy podlegających wymaganiom prawnym lub regulacyjnym

2.2 Obszary zgodności objęte niniejszą polityką obejmują między innymi:

2.2.1 Obowiązki z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa (np. ISO/IEC 27001, NIS2, DORA)

2.2.2 Przepisy dotyczące ochrony danych i prywatności (np. RODO, sektorowe przepisy dotyczące prywatności)

2.2.3 Regulacje sektorowe (np. finansowe, medyczne, motoryzacyjne, obronne)

2.2.4 Zobowiązania umowne wynikające z umów o zachowaniu poufności, umów o poziomie usług (SLA) lub umów dotyczących przetwarzania przez strony trzecie

2.2.5 Wymogi prawne związane ze zgłaszaniem incydentów, współpracą z organami ścigania oraz międzynarodowym transferem danych

3. Cele

3.1 Zapewnienie, że wszystkie mające zastosowanie przepisy prawa, regulacje, normy i zobowiązania umowne są identyfikowane, dokumentowane, interpretowane i egzekwowane w całej organizacji.

3.2 Integracja wymagań prawnych i regulacyjnych z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI), procesami zarządzania ryzykiem, umowami z dostawcami oraz projektowaniem produktów i usług.

3.3 Zapewnienie mechanizmu proaktywnego monitorowania zmian regulacyjnych oraz odpowiedniej aktualizacji środków kontrolnych i dokumentacji.

3.4 Określenie jednoznacznej odpowiedzialności za nadzór nad zgodnością, eskalację naruszeń, obsługę wyjątków oraz raportowanie zewnętrzne.

3.5 Zapewnienie możliwości prześledzenia audytowego i obrony stanowiska organizacji w zakresie zgodności prawnej i regulacyjnej podczas kontroli, dochodzeń lub przeglądów certyfikacyjnych.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Ponoszą strategiczną odpowiedzialność za zgodność z wymaganiami prawnymi i regulacyjnymi w całej organizacji.

4.1.2 Dokonuje przeglądu i zatwierdza decyzje dotyczące zgodności obarczone wysokim ryzykiem, w tym akceptację ryzyka oraz spory prawne.

4.2 Oficer ds. zgodności / doradca prawny

4.2.1 Utrzymuje rejestr obowiązków zgodności, zawierający wszystkie mające zastosowanie przepisy prawa, normy, certyfikacje i klauzule umowne.

4.2.2 Przeprowadza oceny skutków prawnych dla nowych usług, rynków lub przepływów danych.

4.2.3 Zapewnia autorytatywną interpretację przepisów prawa i norm.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 Coroczny przegląd polityki

9.1.1 Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku kalendarzowym w celu:

9.1.1.1 Zapewnienia dalszej zgodności ze zaktualizowanymi przepisami prawa, normami branżowymi i ramami regulacyjnymi

9.1.1.2 Potwierdzenia skuteczności operacyjnej na podstawie ustaleń audytowych i historii incydentów

9.1.1.3 Odzwierciedlenia zmian organizacyjnych (np. nowych jurysdykcji, systemów lub linii biznesowych)

9.2 Przeglądy inicjowane zdarzeniem

9.2.1 Przeglądy doraźne muszą być inicjowane, gdy:

9.2.2 Wprowadzono nowy wymóg prawny lub regulacyjny albo zaktualizowano istniejący

9.2.3 Incydent zgodności lub audyt ujawnił braki w polityce

9.2.4 Organizacja wchodzi na nowy rynek lub uruchamia nową linię usług podlegającą odrębnym ramom zgodności

9.2.5 Trendy egzekwowania lub wytyczne organów regulacyjnych wskazują na zmianę profilu ryzyka

9.3 Własność i zatwierdzanie

9.3.1 Dział prawny oraz Oficer ds. zgodności ponoszą wspólną odpowiedzialność za koordynację procesu przeglądu.

9.3.2 Ostateczne zmiany niniejszej polityki muszą zostać zatwierdzone przez kierownictwo wykonawcze i zarejestrowane w rejestrze zmian polityki wraz z odpowiednimi odniesieniami do kontroli zmian oraz planami komunikacji.

9.4 Kontrola wersji i komunikacja

9.4.1 Każda zaktualizowana wersja niniejszej polityki musi:

9.4.1.1 Zawierać podsumowanie kluczowych zmian

9.4.1.2 Zostać ponownie rozpowszechniona oficjalnymi kanałami (np. portal polityk, LMS, biuletyny wewnętrzne)

9.4.1.3 Wymagać potwierdzenia zapoznania się od personelu, którego dotyczy, w szczególności pełniącego role prawne, operacyjne, bezpieczeństwa oraz zarządzania dostawcami

10. Powiązane polityki i zależności

10.1 Niniejsza polityka funkcjonuje łącznie z następującymi politykami w ramach SZBI organizacji i wzmacnia ich stosowanie:

10.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia bazowe zasady ładu organizacyjnego zapewniające, że wszystkie polityki bezpieczeństwa informacji — w tym dotyczące zgodności — są zgodne ze strategicznymi celami biznesowymi i wymaganiami regulacyjnymi.

10.1.2 P2 – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: definiuje uprawnienia decyzyjne, w tym role prawne i role ds. zgodności odpowiedzialne za nadzór regulacyjny i rozliczalność.

10.1.3 P6 – Polityka zarządzania ryzykiem: wspiera ocenę, przypisanie odpowiedzialności i ograniczanie ryzyk zgodności prawnej i regulacyjnej w całej organizacji.

10.1.4 P8 – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że cały personel zna swoje obowiązki w zakresie zgodności i otrzymuje szkolenie odpowiednie do pełnionej roli.

10.1.5 P12 – Polityka zarządzania aktywami: wzmacnia obowiązki prawne dotyczące zarządzania i ochrony aktywów objętych regulacjami lub wymaganiami umownymi, w tym aktywów związanych z danymi osobowymi i infrastrukturą krytyczną.

10.1.6 P30 – Polityka reagowania na incydenty (P30): reguluje obowiązkowe zgłoszenia prawne (np. art. 33 RODO) oraz procedury eskalacji w przypadku naruszenia zgodności lub zdarzenia regulacyjnego.

10.1.7 P33 – Polityka monitorowania audytu i zgodności: określa ustrukturyzowane działania zapewniające, w tym testowanie kontroli i gromadzenie dowodów, wymagane do wewnętrznej i zewnętrznej weryfikacji zgodności.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 4.2 – Zrozumienie potrzeb i oczekiwań stron zainteresowanych: wymaga identyfikacji i integracji wymagań prawnych i regulacyjnych z SZBI.

11.1.2 Klauzula 5.1 – Przywództwo i zaangażowanie: nakłada na kierownictwo odpowiedzialność za ustanowienie i utrzymywanie zgodności prawnej w całej organizacji.

11.1.3 Klauzula 5.3 – Role organizacyjne, odpowiedzialności i uprawnienia: zapewnia jednoznaczność ról w zakresie nadzoru prawnego i zgodności regulacyjnej.

11.1.4 Załącznik A, środek kontrolny 5.36 – Zgodność z wymaganiami prawnymi i umownymi: ustanawia wymóg identyfikacji i realizacji obowiązków wynikających z przepisów prawa, regulacji i umów.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 5.36: zawiera wytyczne wdrożeniowe dotyczące utrzymywania rejestru obowiązków zgodności, walidacji wymagań regulacyjnych oraz zapewnienia uporządkowanego przechowywania dowodów.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Polityka i procedury planowania bezpieczeństwa: wymaga, aby wymagania zgodności były osadzone w strukturach ładu organizacyjnego i dokumentacji.

11.3.2 PM-1 – Plan programu bezpieczeństwa informacji: nakazuje uwzględnienie środków kontrolnych regulacyjnych jako elementu szerszego programu bezpieczeństwa.

11.3.3 CA-7 – Ciągłe monitorowanie zgodności: wspiera nadzór nad skutecznością kontroli w spełnianiu wymagań prawnych i polityk.

11.3.4 AU-9 – Ochrona informacji audytowych: zapewnia, że logi audytowe i zapisy dotyczące zgodności są chronione i dostępne do kontroli.

11.4 RODO UE (2016/679)

11.4.1 Artykuł 5 – Zasady dotyczące przetwarzania: wymaga zgodnego z prawem przetwarzania informacji, przejrzystości i rozliczalności.

11.4.2 Artykuł 6 – Zgodność z prawem przetwarzania: wymaga stosowania odpowiednich podstaw prawnych dla wszystkich działań związanych z danymi.

11.4.3 Artykuł 24 – Odpowiedzialność administratora: ustanawia bezpośrednią odpowiedzialność za zapewnienie zgodności regulacyjnej.

11.4.4 Artykuł 32 – Bezpieczeństwo przetwarzania: wymaga wdrożenia odpowiednich zabezpieczeń technicznych i organizacyjnych.

11.4.5 Artykuł 33 – Zgłoszenie naruszenia: wymaga, aby naruszenia ochrony danych osobowych były zgłaszane właściwym organom w ciągu 72 godzin.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuły 20–21: wymagają od podmiotów kluczowych i ważnych wdrożenia udokumentowanego ładu organizacyjnego, strategii zgodności prawnej oraz ciągłego przeglądu ryzyk prawnych.

11.6 Rozporządzenie UE DORA (2022/2554)

11.6.1 Artykuł 5(2) – Ramy zarządzania ryzykiem ICT: wymaga integracji zgodności prawnej z szerszymi funkcjami zarządzania ryzykiem i nadzoru.

11.6.2 Artykuł 19 – Ryzyko ICT stron trzecich: nakłada szczególne wymagania prawne dotyczące zarządzania zobowiązaniami umownymi i regulacyjnymi związanymi z zewnętrznymi dostawcami i platformami.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: uwzględnia zgodność prawną i regulacyjną jako krytyczny element ładu organizacyjnego ryzykiem w przedsiębiorstwie.

11.7.2 MEA03 – Monitor Compliance with External Requirements: definiuje bieżące monitorowanie, obsługę wyjątków oraz gotowość do audytu dla wszystkich form obowiązków regulacyjnych.