					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P37S					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**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Zabezpieczenie 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
RODO	Artykuły 5, 6, 32, 33	
Dyrektywa NIS2	Artykuły 21(2)(a), 21(2)(f), 23	
Rozporządzenie DORA	Artykuły 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Cel

1.1 Niniejsza polityka określa podejście organizacji do identyfikowania, spełniania oraz wykazywania zgodności z obowiązkami prawnymi, regulacyjnymi i umownymi.

1.2 Określa jednoznaczne odpowiedzialności oraz praktyczne działania wspierające działalność biznesową w realizacji obowiązków zgodności, w tym wynikających z przepisów o ochronie danych, ram cyberbezpieczeństwa, umów z klientami oraz norm certyfikacyjnych.

1.3 Zapewnia, że nawet bez dedykowanych zespołów ds. zgodności organizacja może prowadzić działalność zgodnie z prawem, właściwie reagować na incydenty oraz utrzymywać gotowość audytową.

1.4 Niniejsza polityka ma kluczowe znaczenie dla uzyskania certyfikacji ISO/IEC 27001:2022 oraz spełnienia oczekiwań klientów zewnętrznych, organów regulacyjnych i partnerów.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników, wykonawców, osób świadczących pracę na innej podstawie oraz dostawców zewnętrznych,

2.1.2 wszystkich usług, operacji, systemów i działań związanych z przetwarzaniem danych, w odniesieniu do których organizacja musi spełniać wymagania prawne lub umowne,

2.1.3 wszystkich lokalizacji i urządzeń wykorzystywanych do przetwarzania informacji biznesowych, niezależnie od tego, czy są używane w biurze, w pracy zdalnej, czy jako zasoby hostowane w chmurze.

2.2 Polityka obejmuje:

2.2.1 przepisy o ochronie danych, takie jak RODO,

2.2.2 regulacje z zakresu cyberbezpieczeństwa, takie jak Dyrektywa NIS2,

2.2.3 obowiązki sektorowe, jeżeli mają zastosowanie,

2.2.4 umowy z klientami, umowy o zachowaniu poufności oraz klauzule audytowe,

2.2.5 dobrowolne certyfikacje, np. ISO 27001, oraz polityki wewnętrzne, które muszą być egzekwowane w celu zapewnienia zgodności.

3. Cele

3.1 Ustanowienie rozliczalności: przypisanie jednoznacznej odpowiedzialności za monitorowanie, aktualizowanie i egzekwowanie obowiązków prawnych, regulacyjnych i umownych.

3.2 Ochrona organizacji: minimalizacja ryzyka naruszeń prawa, kar finansowych, incydentów naruszenia bezpieczeństwa danych oraz szkód reputacyjnych.

3.3 Zapewnienie gotowości audytowej: utrzymywanie możliwych do zweryfikowania zapisów potwierdzających sposób spełniania przez organizację obowiązków zgodności.

3.4 Wsparcie integracji polityk: zapewnienie, że obowiązki prawne i regulacyjne są spójnie wdrażane we wszystkich politykach i procesach.

3.5 Przejrzyste zarządzanie wyjątkami: zapewnienie, że wszelkie wyjątki dotyczące zgodności są dokumentowane, uzasadniane i zatwierdzane w celu ograniczenia ryzyka odpowiedzialności.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Ponosi ogólną odpowiedzialność za zgodność organizacji z wymaganiami prawnymi i regulacyjnymi.

4.1.2 Utrzymuje Rejestr zgodności i zapewnia jego aktualność.

4.1.3 Dokonuje przeglądu umów z klientami oraz zapewnia śledzenie i egzekwowanie szczególnych obowiązków.

4.1.4 Zatwierdza wyjątki od obowiązków zgodności wyłącznie wtedy, gdy są one prawnie uzasadnione i wdrożono środki kompensujące.

4.2 Doradcy zewnętrzni, np. doradca prawny, konsultanci IT lub konsultanci ds. zgodności

4.2.1 Wspierają GM w identyfikowaniu mających zastosowanie przepisów, certyfikacji i obowiązków, np. RODO, NIS2, ISO 27001.

4.2.2 Udzielają wytycznych dotyczących interpretacji nowych regulacji lub zmian w obowiązujących przepisach.

4.2.3 Mogą wspierać aktualizację polityk, audyty lub reagowanie na naruszenia, gdy występuje ryzyko prawne.

[... 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 Planowy coroczny przegląd

9.1.1 Niniejsza polityka musi być poddawana przeglądowi co 12 miesięcy przez GM.

9.1.2 Przegląd musi potwierdzać:

9.1.2.1 adekwatność do aktualnego kontekstu prawnego i umownego,

9.1.2.2 prawidłowe odzwierciedlenie umów z klientami i obowiązków związanych ze świadczeniem usług,

9.1.2.3 spójność z Rejestrem zgodności i innymi politykami.

9.2 Aktualizacje wynikające ze zdarzeń

9.2.1 Niezwłoczny przegląd jest wymagany, jeżeli:

9.2.1.1 zaczyna obowiązywać nowy przepis lub regulacja, np. nowa zasada ochrony danych,

9.2.1.2 klient dodaje do umowy złożone warunki zgodności,

9.2.1.3 wystąpi naruszenie lub incydent niezgodności,

9.2.1.4 firma rozszerza działalność na nowy rynek lub do sektora regulowanego.

9.3 Zatwierdzanie aktualizacji i kontrola wersji

9.3.1 Wszystkie aktualizacje muszą być dokumentowane, wersjonowane i zatwierdzane przez GM.

9.3.2 Wersje historyczne muszą być przechowywane do celów audytowych i prawnych.

9.4 Komunikowanie zmian

9.4.1 Personel i wykonawcy muszą zostać poinformowani o zmianach polityki w ciągu 5 dni roboczych od ich zatwierdzenia.

9.4.2 Wszyscy dostawcy, których dotyczą zmiany, muszą również potwierdzić przyjęcie zaktualizowanych warunków przed dalszym świadczeniem usług.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest wspierana i egzekwowana przez następujące polityki SME:

10.1.1 P3S – Polityka dopuszczalnego użytkowania: zapobiega zachowaniom, które mogą naruszać wymagania prawne lub umowne, np. nieautoryzowanemu udostępnianiu plików.

10.1.2 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: podnosi świadomość personelu w zakresie obowiązków zgodności oraz sposobów unikania naruszeń.

10.1.3 P14S – Polityka retencji i utylizacji danych: zapewnia zgodne z prawem praktyki postępowania z danymi w całym cyklu życia danych.

10.1.4 P17S – Polityka ochrony danych i prywatności: spełnia wymagania RODO oraz wymagania klientów dotyczące postępowania z danymi.

10.1.5 P30S – Polityka reagowania na incydenty: określa sposób reagowania na naruszenia bezpieczeństwa danych lub niespełnienie wymagań zgodności, w tym terminy zgłoszeń.

10.1.6 P36S – Polityka mediów społecznościowych i komunikacji zewnętrznej: zapewnia, że komunikacja publiczna nie narusza obowiązków prawnych ani regulacyjnych.

10.2 Każda powiązana polityka egzekwuje część ram zgodności prawnej i musi być stosowana łącznie z pozostałymi.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1 – Działania odnoszące się do ryzyk i szans: obejmuje ryzyka zgodności.

11.1.2 Klauzula 8.1 – Planowanie operacyjne i nadzór operacyjny: wymaga realizacji procesów spełniających wymagania prawne i umowne.

11.2 ISO/IEC 27002

11.2.1 Zabezpieczenie 5.36 – wskazuje organizacji sposób utrzymywania zapisów obowiązków oraz zapewniania właściwej reakcji na wymagania prawne i regulacyjne.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Polityka i procedury: wymaga formalnych polityk zgodności.

11.3.2 PM-1 – Plan programu bezpieczeństwa informacji: wymaga integracji zgodności prawnej z planowaniem bezpieczeństwa.

11.3.3 CA-1 – Ocena, autoryzacja i monitorowanie.

11.3.4 AU-1 – Polityka audytu: wymaga utrzymywania dowodów zgodności.

11.4 RODO

11.4.1 Artykuł 5 – Zasady przetwarzania danych, w tym rozliczalność.

11.4.2 Artykuł 6 – Podstawa prawna przetwarzania.

11.4.3 Artykuł 32 – Bezpieczeństwo przetwarzania.

11.4.4 Artykuł 33 – Zgłoszenie naruszenia w terminie 72 godzin.

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21(2)(a) i (f) – Polityki wewnętrzne dotyczące ryzyka i nadzoru regulacyjnego.

11.5.2 Artykuł 23 – Egzekwowanie i kary za niespełnienie wymagań zgodności.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 5(2) – Nadzór nad zarządzaniem ryzykiem ICT.

11.6.2 Artykuł 9(1) – Wewnętrzny ład organizacyjny w zakresie zgodności.

11.6.3 Artykuł 17 – Uzgodnienia umowne z dostawcami usług ICT.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: zapewnia śledzenie i adresowanie ryzyk zgodności.

11.7.2 APO13 – Managed Security: obejmuje oparte na ryzyku egzekwowanie zgodności regulacyjnej i umownej.

11.7.3 DSS01 – Managed Operations: wymaga gotowości operacyjnej do spełniania obowiązków prawnych.