					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P17S					Tytuł dokumentu: **Polityka ochrony danych i prywatności**							
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, 6.1.3, 8	
ISO/IEC 27002:2022	Środki kontrolne 5.34, 8.10–8	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
RODO	Artykuły 5, 6, 12–23, 30, 32–34	
Dyrektywa NIS2	Artykuł 21(2)(e), 21(2)(f)	
Rozporządzenie DORA	Artykuły 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Cel

1.1. Niniejsza polityka określa sposób, w jaki organizacja chroni dane osobowe zgodnie z obowiązkami prawnymi, wymogami regulacyjnymi oraz międzynarodowymi normami bezpieczeństwa.

1.2. Zapewnia, że dane osobowe — niezależnie od tego, czy dotyczą klientów, personelu, czy partnerów — są zbierane, wykorzystywane, przechowywane i usuwane w sposób zgodny z prawem, rzetelny i bezpieczny.

1.3. Niniejsza polityka zapewnia również zgodność z ISO/IEC 27001:2022 oraz wspiera gotowość audytową poprzez stosowanie spójnego, opartego na ryzyku podejścia do ochrony prywatności.

1.4. Poprzez niniejszą politykę organizacja wykazuje rozliczalność i buduje zaufanie klientów, nadając priorytet przejrzystości, minimalizacji danych oraz skutecznemu nadzorowi nad prywatnością.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do:

2.1.1. wszystkich pracowników, wykonawców i usługodawców, którzy uzyskują dostęp do danych osobowych, przetwarzają je lub nimi zarządzają,

2.1.2. wszystkich systemów, aplikacji i lokalizacji, w których dane osobowe są przechowywane lub przesyłane,

2.1.3. wszystkich danych osobowych, niezależnie od tego, czy są przechowywane elektronicznie, w formie papierowej, w systemach chmurowych czy na urządzeniach mobilnych.

2.2. Niniejsza polityka ma zastosowanie do danych dotyczących klientów, personelu, dostawców oraz wszelkich innych osób możliwych do zidentyfikowania.

2.3. Polityka obowiązuje niezależnie od tego, czy dane są przetwarzane wewnętrznie, czy przez zewnętrznych dostawców usług.

3. Cele

3.1. Zapewnienie, że dane osobowe są przetwarzane zgodnie z przepisami o ochronie prywatności i normami bezpieczeństwa, w tym RODO, NIS2 i ISO 27001.

3.2. Ochrona danych osobowych przed nieuprawnionym dostępem, niewłaściwym wykorzystaniem, modyfikacją lub utratą poprzez wdrożenie jednoznacznych zabezpieczeń technicznych i organizacyjnych.

3.3. Poszanowanie praw osób, których dane dotyczą, w tym prawa dostępu do danych, ich sprostowania i usunięcia.

3.4. Ustanowienie jasnych ról i odpowiedzialności w zakresie ochrony danych w organizacji.

3.5. Zapewnienie minimalizacji danych, bezpiecznych okresów przechowywania oraz terminowego usuwania we wszystkich systemach i procesach.

3.6. Ograniczenie ryzyka niezgodności, sankcji prawnych, szkód reputacyjnych lub utraty zaufania klientów.

4. Role i obowiązki

4.1. Dyrektor Generalny (GM)

4.1.1. Zatwierdza niniejszą politykę i zapewnia jej stosowanie.

4.1.2. Zapewnia niezbędne zasoby do zarządzania ryzykiem związanym z prywatnością i reagowania na incydenty.

4.1.3. Ponosi ogólną odpowiedzialność za zgodność z przepisami i normami dotyczącymi prywatności.

4.2. Koordynator ds. prywatności (wewnętrzny lub zewnętrzny)

4.2.1. Utrzymuje rejestr czynności przetwarzania.

4.2.2. Odpowiada na wnioski osób, których dane dotyczą, oraz zapytania organów regulacyjnych.

4.2.3. Wspiera ocenę ryzyka, szkolenia i wdrożenie polityki.

4.2.4. Dokumentuje przypadki naruszeń i zgłasza je właściwym organom, jeśli jest to wymagane.

[... 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. Planowane przeglądy

9.1.1. Niniejsza polityka musi być poddawana przeglądowi co najmniej raz na 12 miesięcy przez Koordynatora ds. prywatności i zatwierdzana przez Dyrektora Generalnego.

9.1.2. Przegląd musi obejmować ocenę aktualności polityki, zgodności regulacyjnej oraz skuteczności operacyjnej.

9.2. Przesłanki przeglądu doraźnego

9.2.1. Aktualizacja polityki musi być również inicjowana w odpowiedzi na:

9.2.1.1. nowe lub znowelizowane przepisy dotyczące ochrony danych (np. RODO, DORA),

9.2.1.2. incydenty bezpieczeństwa lub naruszenia prywatności dotyczące danych osobowych,

9.2.1.3. uruchomienie nowych systemów, narzędzi lub usług przetwarzających dane osobowe,

9.2.1.4. istotne ustalenia audytowe lub zalecenia organów regulacyjnych.

9.3. Kontrola zmian i komunikacja

9.3.1. Wszystkie zmiany w polityce muszą być formalnie dokumentowane w dzienniku zmian.

9.3.2. Zmienione wersje muszą być przekazywane całemu personelowi oraz właściwym wykonawcom.

9.3.3. Wersje archiwalne muszą być przechowywane na potrzeby ścieżki audytowej zgodności.

10. Powiązane polityki i zależności

10.1. Niniejsza polityka funkcjonuje łącznie z innymi politykami SME w celu ustanowienia kompletnej i wykonalnej struktury ochrony prywatności:

10.1.1. P13S – Polityka klasyfikacji i oznaczania informacji: zapewnia odpowiednią klasyfikację danych osobowych, tak aby środki ochrony prywatności mogły być stosowane adekwatnie do poziomu ryzyka.

10.1.2. P14S – Polityka retencji i utylizacji danych: określa jasne zasady dotyczące okresu przechowywania danych osobowych oraz bezpiecznych metod ich utylizacji po upływie wymaganego okresu.

10.1.3. P16S – Polityka maskowania danych i pseudonimizacji: określa, w jaki sposób identyfikatory osobowe muszą być przekształcane przed wykorzystaniem danych w środowiskach nieprodukcyjnych lub przed ich udostępnieniem na zewnątrz.

10.1.4. P30S – Polityka reagowania na incydenty: obejmuje działania wymagane przy reagowaniu na naruszenia ochrony danych, w tym zgłaszanie ich organom regulacyjnym i osobom, których dane dotyczą, w wymaganych terminach.

10.1.5. P2S – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: doprecyzowuje strukturę odpowiedzialności i role decyzyjne mające zastosowanie do wdrażania i nadzoru nad ochroną prywatności.

10.2. Powiązane polityki muszą być przeglądane i stosowane łącznie w celu zapewnienia pełnej ochrony prywatności w systemach, w odniesieniu do personelu i dostawców.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 5.1 – wymaga od najwyższego kierownictwa wykazania przywództwa i zaangażowania w ochronę danych osobowych.

11.1.2. Klauzula 6.1.3 – nakłada obowiązek postępowania z ryzykami związanymi z przetwarzaniem danych osobowych.

11.1.3. Klauzula 8.1 – wymaga wdrożenia zabezpieczeń operacyjnych w celu ochrony danych w całym ich cyklu życia.

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 5.34 – zawiera wytyczne wdrożeniowe dotyczące ochrony prywatności i bezpiecznego postępowania z danymi osobowymi.

11.2.2. Środek kontrolny 8.10 – dotyczy bezpiecznej utylizacji danych osobowych w celu zapobiegania ich resztkowemu ujawnieniu.

11.2.3. Środek kontrolny 8.11 – wspiera stosowanie maskowania i pseudonimizacji na potrzeby minimalizacji danych.

11.2.4. Środek kontrolny 8.12 – zapobiega nieuprawnionym wyciekom danych poprzez kontrolę dostępu do danych i zasad ich wykorzystania.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2 – przypisuje role i odpowiedzialności za zarządzanie ryzykiem w obszarze prywatności.

11.3.2. PL-5 – wymaga dokumentacji planu prywatności obejmującego wykorzystanie i ochronę danych.

11.3.3. AC-6 – nakłada wymóg stosowania zasady najmniejszych uprawnień i kontroli dostępu do danych osobowych.

11.3.4. IR-4 – wymaga procesów obsługi incydentów w przypadku naruszeń dotyczących danych osobowych.

11.4. RODO

11.4.1. Artykuł 5 – określa podstawowe zasady zgodnego z prawem, rzetelnego i przejrzystego przetwarzania danych.

11.4.2. Artykuł 6 – wymaga istnienia ważnej podstawy prawnej dla każdej czynności przetwarzania danych osobowych.

11.4.3. Artykuły 12–23 – określają prawa osób, których dane dotyczą, w tym prawo dostępu, sprostowania, usunięcia i sprzeciwu.

11.4.4. Artykuł 30 – nakłada obowiązek prowadzenia rejestru czynności przetwarzania.

11.4.5. Artykuł 32 – wymaga stosowania odpowiednich zabezpieczeń technicznych i organizacyjnych.

11.4.6. Artykuły 33–34 – określają obowiązki zgłaszania naruszeń organom i osobom, których dane dotyczą.

11.5. Dyrektywa NIS2

11.5.1. Artykuł 21(2)(e) – wymaga stosowania środków zapewniających ochronę danych zgodnie z politykami cyberbezpieczeństwa.

11.5.2. Artykuł 21(2)(f) – nakłada obowiązek stosowania mechanizmów zarządzania bezpieczeństwem danych osobowych i informacji poufnych w systemach ICT.

11.6. Rozporządzenie DORA

11.6.1. Artykuł 6 – wymaga wewnętrznych ram ładu organizacyjnego umożliwiających zarządzanie ryzykiem danych i ich ochroną.

11.6.2. Artykuł 15 – zobowiązuje podmioty finansowe do zapewnienia, że dostawcy zewnętrzni chronią dane osobowe i wspierają zgodność regulacyjną.

11.6.3. Artykuł 17 – wymaga zapewnienia, że systemy ICT przetwarzające dane osobowe są bezpieczne, odporne i monitorowane.

11.7. COBIT 2019

11.7.1. APO12 – Zarządzanie ryzykiem: wymaga identyfikacji ryzyk dotyczących prywatności i ochrony danych oraz odpowiedniego postępowania z nimi.

11.7.2. DSS05 – Zarządzanie usługami bezpieczeństwa: nakłada obowiązek stosowania zabezpieczeń zapobiegających nieuprawnionemu dostępowi do danych osobowych.

11.7.3. MEA03 – Monitorowanie zgodności: wymaga, aby organizacje zapewniały ciągłą zgodność z przepisami dotyczącymi prywatności i ochrony danych.