					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P17					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, 8.1, 10	Odpowiednie ogólne, techniczne oraz dotyczące ciągłego doskonalenia środki kontrolne w zakresie ochrony danych
ISO/IEC 27002:2022	Środki kontrolne 5.34, 8.10, 8.11, 8.12	Środki kontrolne dotyczące postępowania z danymi osobowymi, retencji, usuwania, anonimizacji oraz praw osób, których dane dotyczą
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Wymagania dotyczące ładu organizacyjnego, ryzyka, zarządzania dostępem, rejestrowania, reagowania na naruszenia oraz programu prywatności
RODO	Artykuły 5, 6, 12–23, 25, 28, 30, 32–34; motyw 78	Wszystkie kluczowe wymagania dotyczące prywatności, rozliczalności, praw osób, których dane dotyczą, realizacji żądań, naruszeń oraz zasad ochrony danych w fazie projektowania i domyślnej ochrony danych
Dyrektywa NIS2	Artykuł 21(2)(e), (f)	Oparte na ryzyku środki bezpieczeństwa dla podmiotów kluczowych i ważnych
Rozporządzenie DORA	Artykuły 6(2)(d), 11(1)(c), 15(1), 17	Ład organizacyjny, ryzyko stron trzecich oraz wymagania bezpiecznego przetwarzania
COBIT 2019	APO12, DSS01, DSS05, MEA	Zarządzanie ryzykiem, bezpieczne operacje, nadzór nad zgodnością

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe zasady organizacyjne oraz wymagania techniczne dotyczące ochrony danych osobowych i stosowania zasad privacy by design we wszystkich środowiskach.

1.2 Formalizuje ona odpowiedzialność organizacji wynikającą z norm międzynarodowych i ram regulacyjnych, zapewniając, że dane osobowe są zbierane, przetwarzane, przechowywane, udostępniane i usuwane zgodnie z prawem, bezpiecznie i w sposób przejrzysty.

1.3 Niniejsza polityka wzmacnia również zgodność z mającymi zastosowanie przepisami i ramami dotyczącymi prywatności, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), dyrektywą NIS2, rozporządzeniem DORA, ISO/IEC 27001:2022 oraz COBIT 2019.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich jednostek organizacyjnych, członków personelu i systemów zaangażowanych w przetwarzanie danych osobowych, w tym:

2.1.1 pracowników, kontraktorów, konsultantów i dostawców usług zewnętrznych.

2.1.2 danych pozyskiwanych ze źródeł wewnętrznych i zewnętrznych we wszystkich funkcjach biznesowych.

2.1.3 nośników fizycznych i cyfrowych, w tym usług chmurowych, platform SaaS, urządzeń mobilnych oraz dokumentacji papierowej.

2.1.4 wszystkich środowisk, w tym produkcyjnych, deweloperskich, testowych i środowisk kopii zapasowych, w których mogą występować dane osobowe.

2.2 Obejmuje ona wszystkie czynności przetwarzania regulowane przez mające zastosowanie przepisy i normy dotyczące prywatności, w tym między innymi:

2.2.1 zbieranie, przechowywanie, wykorzystywanie, przesyłanie oraz usuwanie danych osobowych.

2.2.2 realizację praw osób, których dane dotyczą, dokumentowanie podstawy prawnej oraz zarządzanie zgodą.

2.2.3 transfery transgraniczne, zgłaszanie naruszeń oraz udostępnianie danych stronom trzecim.

2.2.4 bezpieczne projektowanie oraz domyślne zapewnianie ochrony prywatności w systemach i procesach.

3. Cele

3.1 Zapewnienie zgodnego z prawem, przejrzystego i rozliczalnego przetwarzania danych osobowych zgodnie z ISO/IEC 27001:2022 oraz powiązanymi wymaganiami prawnymi.

3.2 Wbudowanie zasad privacy by design i privacy by default we wszystkie systemy informatyczne organizacji, usługi i procesy biznesowe.

3.3 Egzekwowanie technicznych i organizacyjnych środków ochrony, które zapewniają poufność, integralność i dostępność (CIA) danych osobowych przez cały ich cykl życia.

3.4 Określenie ról w zakresie ładu organizacyjnego i struktur rozliczalności dotyczących ochrony danych, w tym odpowiedzialności inspektora ochrony danych, zespołu ds. bezpieczeństwa informacji, funkcji prawnej i zgodności oraz właścicieli danych.

3.5 Zapewnienie pełnej zgodności z artykułami 5, 6, 25, 30 i 32 RODO, a także z wymaganiami dotyczącymi ograniczania ryzyka i odporności wynikającymi z NIS2 i DORA.

3.6 Zapewnienie realizacji praw osób, których dane dotyczą, w tym prawa dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu oraz ochrony przed zautomatyzowanym podejmowaniem decyzji.

3.7 Ograniczanie ryzyka regulacyjnego, reputacyjnego, prawnego i operacyjnego wynikającego z nieuprawnionego dostępu, niewłaściwego wykorzystania lub utraty danych osobowych.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zapewnia strategiczny nadzór i przydziela wystarczające zasoby na potrzeby programu prywatności.

4.1.2 Zatwierdza niniejszą politykę i zapewnia jej stosowanie w całej organizacji.

4.2 Inspektor ochrony danych

4.2.1 Działa niezależnie w celu nadzorowania zgodności z przepisami o ochronie danych.

4.2.2 Utrzymuje rejestr czynności przetwarzania (RoPA) zgodnie z art. 30 RODO.

4.2.3 Kieruje współpracą z organami nadzorczymi, przeprowadza oceny skutków dla ochrony danych (DPIA) oraz zarządza procesami zgłaszania naruszeń.

4.2.4 Dokonuje przeglądu odstępstw dotyczących prywatności i utrzymuje rejestr odstępstw dotyczących prywatności.

[... 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 Niniejsza polityka musi podlegać przeglądowi co najmniej raz w roku lub wcześniej w następujących przypadkach:

9.1.1 istotnych zmian prawnych lub regulacyjnych (np. zmian w RODO, terminów DORA),

9.1.2 wdrożenia nowych systemów lub czynności przetwarzania obejmujących dane osobowe,

9.1.3 ustaleń audytu wewnętrznego wskazujących na luki w polityce,

9.1.4 istotnych incydentów naruszeń lub informacji zwrotnych od organu nadzorczego.

9.2 Odpowiedzialność za przegląd

9.2.1 Inspektor ochrony danych inicjuje przegląd polityki, koordynując działania z funkcją prawną i zgodności, funkcją ryzyka, bezpieczeństwa informacji oraz kierownictwem wykonawczym.

9.2.2 Wszystkie aktualizacje muszą być rejestrowane w rejestrze kontroli dokumentów SZBI i przekazywane zainteresowanym stronom, których dotyczą.

9.3 Kontrola zmian

9.3.1 Każda zmiana niniejszej polityki musi zostać formalnie zatwierdzona przez kierownictwo wykonawcze.

9.3.2 Nieaktualne wersje muszą być archiwizowane w sposób bezpieczny, a zaktualizowana wersja musi zawierać udokumentowaną historię zmian.

10. Powiązane polityki i zależności

10.1 P1 – Polityka bezpieczeństwa informacji. Określa nadrzędne zasady ładu bezpieczeństwa stanowiące podstawę niniejszej polityki prywatności. P1 wspiera poufność, integralność i dostępność (CIA) danych osobowych we wszystkich systemach i usługach.

10.2 P6 – Polityka zarządzania ryzykiem. Określa metodykę postępowania z ryzykiem w organizacji, która jest niezbędna do oceny ryzyk prywatności, prowadzenia DPIA oraz oceny ryzyka rezydualnego wymaganej przez RODO i klauzulę 6.1.3 ISO/IEC 27001.

10.3 P13 – Polityka klasyfikacji danych i etykietowania. Określa zasady kategoryzacji danych osobowych i danych wrażliwych, stanowiące podstawę stosowania odpowiednich mechanizmów ochrony prywatności, w tym egzekwowania retencji, ograniczania dostępu i bezpiecznego usuwania.

10.4 P14 – Polityka retencji i usuwania danych. Bezpośrednio wspiera wymagania dotyczące prywatności wynikające z art. 5 ust. 1 lit. e oraz art. 17 RODO, zapewniając, że dane osobowe są przechowywane wyłącznie przez okres niezbędny i bezpiecznie usuwane zgodnie z obowiązkami prawnymi.

10.5 P16 – Polityka maskowania danych i pseudonimizacji. Ustanawia środki kontrolne ograniczające możliwość identyfikacji danych osobowych za pomocą środków technicznych, takich jak tokenizacja, maskowanie dynamiczne i pseudonimizacja, zapewniając tym samym zgodność z art. 32 RODO oraz środkiem kontrolnym 5.34 normy ISO/IEC 27002.

10.6 P30 – Polityka reagowania na incydenty. Określa obowiązkowe procedury reagowania na naruszenia, zintegrowane z obsługą naruszeń prywatności i terminami zgłoszeń wymaganymi przez art. 33 i 34 RODO.

10.7 P33 – Polityka monitorowania audytu i zgodności. Zapewnia egzekwowanie planowych ocen skuteczności programu prywatności, stosowania polityki oraz śledzenia działań korygujących w jednostkach organizacyjnych i u podmiotów przetwarzających będących stronami trzecimi.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 5.1 – Przywództwo i zaangażowanie: ustanawia odpowiedzialność na poziomie kierowniczym za ochronę danych osobowych i stosowanie zasad prywatności.

11.1.2 Klauzula 6.1.3 – Postępowanie z ryzykiem bezpieczeństwa informacji: wspiera identyfikację, ocenę i postępowanie z ryzykiem prywatności za pomocą DPIA i odstępstw.

11.1.3 Klauzula 8.1 – Planowanie i nadzór operacyjny: wymaga technicznych i proceduralnych środków bezpieczeństwa zapewniających bezpieczne przetwarzanie danych osobowych.

11.1.4 Klauzula 10.1 – Ciągłe doskonalenie: nakłada obowiązek okresowej oceny i dostosowywania programu prywatności.

11.2 ISO/IEC 27002:2022 Środki kontrolne 5.34, 8.10, 8.11, 8.12: zawierają wytyczne dotyczące postępowania z danymi osobowymi, egzekwowania retencji, usuwania, anonimizacji oraz przejrzystości w zakresie praw osób, których dane dotyczą.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: określają ład organizacyjny, role, rozliczalność i obowiązki szkoleniowe w zakresie prywatności.

11.3.2 PL-2, PL-8: wymagają integracji mechanizmów ochrony prywatności z cyklem życia systemu i architekturą organizacji.

11.3.3 AC-2, AC-6: egzekwują zasadę najmniejszych uprawnień oraz zarządzanie kontami na potrzeby ochrony danych osobowych.

11.3.4 AU-2, AU-6, AU-9: nakazują rejestrowanie, identyfikowalność i integralność audytową dostępu do danych osobowych.

11.3.5 IR-4, IR-5, IR-6: określają ustrukturyzowane procesy wykrywania, analizy i zgłaszania naruszeń prywatności.

11.3.6 PM-1, PM-21, PM-23: ustanawiają kompleksowy program prywatności, zgodny ze strategicznymi celami w zakresie ryzyka i ładu danymi.

11.4 RODO (2016/679)

11.4.1 Artykuły 5, 6, 12–23, 25, 28, 30, 32–34: regulują zgodne z prawem przetwarzanie, ograniczenie celu, prawa osób, których dane dotyczą, rozliczalność, ochronę danych w fazie projektowania i domyślną ochronę danych, zobowiązania stron trzecich oraz zarządzanie naruszeniami.

11.4.2 Motyw 78: wzmacnia zasady privacy by design.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(e) i (f): wymaga wdrożenia opartych na ryzyku środków bezpieczeństwa oraz ochrony danych osobowych w podmiotach objętych zakresem jako podmioty kluczowe i ważne.

11.6 Rozporządzenie UE DORA (2022/2554)

11.6.1 Artykuł 6(2)(d): egzekwuje wewnętrzny ład organizacyjny dla zarządzania ryzykiem ICT odnoszącego się do przetwarzania danych.

11.6.2 Artykuł 11(1)(c): nakłada obowiązek nadzoru nad ryzykiem stron trzecich dla usług związanych z danymi.

11.6.3 Artykuły 15(1) i 17: wymagają bezpiecznego przetwarzania danych przez dostawców usług oraz terminowych zgłoszeń nadzorczych po incydentach związanych z ICT.

11.7 COBIT 2019

11.7.1 APO12 – Polityka zarządzania ryzykiem: uwzględnia ryzyko prywatności w szerszym nadzorze nad ryzykiem organizacji.

11.7.2 DSS01 – Zarządzane operacje oraz DSS05 – Zarządzanie usługami bezpieczeństwa: zapewniają bezpieczne operacje, w tym kontrolę dostępu, retencję i integralność systemów.

11.7.3 MEA03 – Monitorowanie zgodności: wymaga ciągłego przeglądu statusu zgodności względem obowiązków dotyczących prywatności wynikających z regulacji i polityk.