					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P16S					Tytuł dokumentu: **Polityka maskowania danych i pseudonimizacji P16S**							
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**

Zgodność z normami i regulacjami

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 6.1.3, Klauzula 8	Ryzyka związane z bezpieczeństwem informacji oraz niezbędne zabezpieczenia, w tym maskowanie i pseudonimizacja
ISO/IEC 27002:2022	Środki kontrolne 8.11, 8.12	Wytyczne dotyczące maskowania oraz zapobiegania wyciekom danych
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Ukrywanie danych oraz technologie zwiększające prywatność
EU NIS2	Artykuł 21(2)(c)	Proporcjonalne środki techniczne, w tym pseudonimizacja jako zabezpieczenie
EU DORA	Artykuł 10(1)	Środki kontroli ryzyka ICT, w tym zabezpieczenia związane z transformacją danych
COBIT 2019	DSS05.01, DSS06	Ochrona danych oraz techniki ukrywania danych i pseudonimizacji
EU GDPR	Artykuły 4(5), 5(1)(c), 32	Minimalizacja danych oraz pseudonimizacja jako techniczny środek kontrolny

1. Cel

1.1. Niniejsza polityka określa wiążące wymagania dotyczące stosowania maskowania danych i pseudonimizacji w celu ochrony danych wrażliwych, danych osobowych i danych poufnych w małych i średnich przedsiębiorstwach (MŚP).

1.2. Techniki te są obowiązkowe wszędzie tam, gdzie rzeczywiste dane nie są niezbędne, w szczególności w środowiskach deweloperskich, na potrzeby analiz lub przy świadczeniu usług przez podmioty trzecie, aby ograniczyć ryzyko ujawnienia, niewłaściwego użycia lub naruszenia bezpieczeństwa.

1.3. Niniejsza polityka bezpośrednio wspiera zgodność z wymaganiami certyfikacyjnymi ISO/IEC 27001:2022 oraz z europejskimi wymogami regulacyjnymi, takimi jak RODO, dyrektywa NIS2 i rozporządzenie DORA.

1.4. Poprzez przekształcanie danych przed ich wykorzystaniem poza pierwotnym kontekstem biznesowym organizacja ogranicza odpowiedzialność oraz zwiększa zdolność do wykazania należytej staranności w zakresie prywatności i bezpieczeństwa.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich danych ustrukturyzowanych i nieustrukturyzowanych sklasyfikowanych jako dane osobowe, poufne lub wrażliwe, niezależnie od tego, czy są przechowywane lub przetwarzane:

2.1.1. W środowiskach produkcyjnych, testowych lub deweloperskich

2.1.2. Na urządzeniach lokalnych, serwerach lub platformach chmurowych

2.1.3. Przez pracowników wewnętrznych, wykonawców lub dostawców zewnętrznych

2.2. Obejmuje ona również wszystkie narzędzia do transformacji danych (maskowanie, tokenizacja, pseudonimizacja), niezależnie od tego, czy są to rozwiązania open source, komercyjne czy opracowane wewnętrznie.

2.3. Przypadki użycia objęte niniejszą polityką obejmują:

2.3.1. Przygotowanie testowych lub deweloperskich zbiorów danych

2.3.2. Eksport danych do systemów analitycznych

2.3.3. Dostęp dostawców lub konsultantów do systemów operacyjnych

2.3.4. Ograniczenie zakresu danych dotyczących osoby, której dane dotyczą, w celu zmniejszenia ryzyka przetwarzania

3. Cele

3.1. Zapewnienie, że rzeczywiste dane osobowe lub dane wrażliwe nigdy nie są ujawniane w środowiskach o niższym poziomie bezpieczeństwa, jeżeli nie jest to niezbędne.

3.2. Wymaganie stosowania maskowania lub pseudonimizacji, gdy rzeczywiste identyfikatory nie są bezwzględnie niezbędne do realizacji zadania.

3.3. Zapobieganie nieuprawnionemu dostępowi do danych lub ich niewłaściwemu użyciu poprzez stosowanie mechanizmów kontroli transformacji przed przekazaniem lub przetwarzaniem danych.

3.4. Zapewnienie, że wszystkie procesy maskowania i pseudonimizacji są audytowalne, podlegają kontroli oraz są realizowane z użyciem zatwierdzonych narzędzi.

3.5. Zapewnienie zgodności z obowiązującymi wymogami prawnymi i regulacyjnymi dotyczącymi minimalizacji danych, poufności oraz zabezpieczeń związanych z transformacją danych.

4. Role i obowiązki

4.1. Dyrektor Generalny (GM)

4.1.1. Odpowiada za niniejszą politykę i zatwierdza ją

4.1.2. Zapewnia, że wszystkie działy i dostawcy przestrzegają wymagań dotyczących transformacji danych

4.1.3. Dokonuje przeglądu wyjątków, ocen ryzyka i rejestrów transformacji

4.1.4. Koordynuje działania prawne, operacyjne oraz działania wobec dostawców w przypadku naruszeń

4.2. Dostawca usług IT / wewnętrzny dział IT

4.2.1. Wybiera i zarządza narzędziami do maskowania lub pseudonimizacji

4.2.2. Zapewnia stosowanie odpowiednich metod transformacji w zależności od rodzaju danych

4.2.3. Utrzymuje rejestry przekształconych zbiorów danych oraz procedury zarządzania kluczami

4.2.4. Zapewnia, że maskowanie jest wykonywane przed wykorzystaniem danych do testów, przez dostawców lub na potrzeby analiz

[... 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

9.1.1. Niniejsza polityka musi być przeglądana co najmniej raz w roku przez Dyrektora Generalnego w celu zapewnienia, że odzwierciedla:

9.1.1.1. Aktualizacje obowiązujących przepisów i regulacji (np. RODO, DORA)

9.1.1.2. Nowe systemy biznesowe lub wymianę danych z podmiotami trzecimi

9.1.1.3. Informacje zwrotne z audytów lub incydentów związanych z wykorzystaniem danych bez maskowania

9.2. Przeglądy doraźne

9.2.1. Przeglądy muszą być również przeprowadzane, gdy:

9.2.1.1. Wprowadzane są nowe aplikacje lub platformy przetwarzające dane wrażliwe

9.2.1.2. Poważny incydent ujawnia luki w obecnych mechanizmach kontroli transformacji

9.2.1.3. Zmiany poziomów klasyfikacji wpływają na procedury postępowania z danymi

9.3. Kontrola wersji i zarządzanie zmianą

9.3.1. Wszystkie zmiany polityki muszą być:

9.3.1.1. Zatwierdzone przez GM i udokumentowane w rejestrze zmian

9.3.1.2. Jednoznacznie zakomunikowane pracownikom i dostawcom usług, których dotyczą

9.3.1.3. Archiwizowane w sposób bezpieczny, z ograniczonym dostępem do nieaktualnych wersji

10. Powiązane polityki i zależności

10.1. Niniejszą politykę należy stosować łącznie z następującymi politykami MŚP, aby zapewnić spójną i egzekwowalną ochronę danych wrażliwych:

10.1.1. P13S – Polityka klasyfikacji i oznaczania danych: Określa poziomy klasyfikacji (np. „Poufne – Dane osobowe”), które decydują o konieczności zastosowania maskowania lub pseudonimizacji. Niniejsza polityka egzekwuje zasady transformacji w zależności od poziomu wrażliwości danych.

10.1.2. P14S – Polityka przechowywania i usuwania danych: Zapewnia, że przekształcone zbiory danych, w tym kopie zapasowe zawierające dane zamaskowane lub spseudonimizowane, są przechowywane i usuwane zgodnie z obowiązującymi zasadami, w tym z usuwaniem kluczy mapowania, gdy nie są już potrzebne.

10.1.3. P17S – Polityka ochrony danych i prywatności: Zapewnia zgodność praktyk transformacji z szerszymi obowiązkami w zakresie prywatności, w tym z wymaganiami RODO dotyczącymi minimalizacji danych i stosowania pseudonimizacji jako środka ochrony przy przetwarzaniu danych osobowych.

10.1.4. P30S – Polityka reagowania na incydenty: Obejmuje procedury zgłaszania i eskalacji w przypadku nieuprawnionego ujawnienia danych, w tym niewłaściwego użycia lub odwrócenia procesu maskowania albo pseudonimizacji.

10.1.5. P2S – Polityka ról i obowiązków w nadzorze: Przypisuje ogólną odpowiedzialność za stosowanie polityki, akceptację ryzyka i zatwierdzanie wyjątków, przede wszystkim Dyrektorowi Generalnemu.

10.2. Polityki te tworzą zintegrowane ramy ochrony danych, zapewniając, że działania związane z maskowaniem i pseudonimizacją wspierają certyfikację ISO 27001 oraz zgodność z wieloma regulacjami.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 6.1.3: Wymaga postępowania z ryzykiem w obszarze bezpieczeństwa informacji, w tym ograniczania ekspozycji poprzez techniki transformacji danych.

11.1.2. Klauzula 8.1: Wymaga wdrożenia środków kontrolnych niezbędnych do osiągnięcia celów bezpieczeństwa, w tym pseudonimizacji i maskowania.

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 8.11: Zawiera wytyczne dotyczące maskowania danych wrażliwych w systemach testowych i deweloperskich.

11.2.2. Środek kontrolny 8.12: Przedstawia metody zapobiegania wyciekowi danych poprzez kontrolowaną transformację i kontrolę dostępu.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Zapewnia poufność informacji poprzez ukrywanie danych.

11.3.2. SC-28: Chroni informacje przechowywane i przetwarzane.

11.3.3. PT-2/PT-3: Promują stosowanie technologii zwiększających prywatność, w tym pseudonimizacji, przy przetwarzaniu danych osobowych.

11.4. EU GDPR

11.4.1. Artykuł 4(5): Definiuje prawnie pseudonimizację i wymaga stosowania mechanizmów kontroli nad kluczami mapowania oraz identyfikatorami.

11.4.2. Artykuł 5(1)(c): Wspiera zasadę minimalizacji danych poprzez maskowanie.

11.4.3. Artykuł 32: Uznaje pseudonimizację za techniczny środek kontrolny ograniczający ryzyka dla prywatności.

11.5. Dyrektywa UE NIS2

11.5.1. Artykuł 21(2)(c): Wymaga proporcjonalnych środków technicznych ograniczających ryzyko dla bezpieczeństwa danych, w tym pseudonimizacji jako elementu kontroli ryzyka.

11.6. Rozporządzenie UE DORA

11.6.1. Artykuł 10(1): Wymaga stosowania środków kontroli ryzyka ICT obejmujących zabezpieczenia transformacji danych na potrzeby ciągłości działania i poufności podczas outsourcingu oraz rozwoju systemów.

11.7. COBIT 2019

11.7.1. DSS05.01: Wymaga ochrony aktywów informacyjnych, w tym transformacji danych tam, gdzie jest to możliwe.

11.7.2. DSS06.06: Wymaga stosowania odpowiednich technik ukrywania danych i pseudonimizacji w celu ograniczenia ekspozycji danych w środowiskach o niższym poziomie zaufania.