POLITYKA OCHRONY DANYCH OSOBOWYCH

WARMEKO Sp. z o.o.

Nazwa dokumentu	Polityka ochrony danych osobowych
Administrator	WARMEKO Sp. z o.o.
Siedziba	ul. Kołobrzeska 50/215, 10-434 Olsztyn
Data przyjęcia	29 września 2026 r.

Cel dokumentu
Ustanowienie zasad zgodnego z prawem, bezpiecznego i rozliczalnego przetwarzania danych osobowych w WARMEKO Sp. z o.o. Polityka wymaga uzupełnienia dokumentami wykonawczymi, w szczególności rejestrem czynności przetwarzania, analizą ryzyka, ewidencją upoważnień i rejestrem naruszeń.

1. Postanowienia ogólne

1. Niniejsza Polityka ochrony danych osobowych, zwana dalej „Polityką", określa zasady przetwarzania i ochrony danych osobowych przez WARMEKO Sp. z o.o. z siedzibą przy ul. Kołobrzeskiej 50/215, 10-434 Olsztyn, zwaną dalej „Administratorem" lub „Spółką".

2. Polityka została ustanowiona w celu zapewnienia zgodności przetwarzania danych z RODO, ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz innymi właściwymi przepisami prawa.

3. Polityka ma charakter dokumentu wewnętrznego i obowiązuje wszystkie osoby przetwarzające dane osobowe z upoważnienia Administratora, niezależnie od podstawy zatrudnienia lub współpracy.

4. Administrator stosuje zasadę rozliczalności i jest zobowiązany nie tylko przestrzegać zasad ochrony danych, lecz także wykazać ich przestrzeganie poprzez odpowiednią dokumentację, zabezpieczenia i dowody realizowanych działań.

5. Polityka podlega okresowym przeglądom oraz aktualizacji w razie zmian prawnych, organizacyjnych, technologicznych lub zmian ryzyka.

2. Podstawy prawne

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO);
- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- przepisy sektorowe właściwe dla działań Spółki, w tym dotyczące rachunkowości, podatków, zatrudnienia, świadczenia usług drogą elektroniczną i komunikacji elektronicznej;
- umowy zawarte przez Administratora, jeżeli określają wymagania dotyczące ochrony danych osobowych.

3. Definicje

Pojęcie	Znaczenie
Administrator	WARMEKO Sp. z o.o., która ustala cele i sposoby przetwarzania danych osobowych.
Dane osobowe	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
Przetwarzanie	operacja lub zestaw operacji wykonywanych na danych, np. zbieranie, utrwalanie, organizowanie, przechowywanie, przeglądanie, wykorzystywanie, udostępnianie lub usuwanie.
Osoba upoważniona	pracownik, współpracownik lub inna osoba dopuszczona przez Administratora do przetwarzania danych.
Podmiot przetwarzający	podmiot, który przetwarza dane osobowe w imieniu Administratora na podstawie umowy lub innego instrumentu prawnego.

Naruszenie ochrony danych	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych.
System informatyczny	sprzęt, oprogramowanie, usługi chmurowe, poczta elektroniczna, strona internetowa, urządzenia mobilne i sieci wykorzystywane do przetwarzania danych.

4. Zakres stosowania Polityki

Polityka obejmuje dane osobowe przetwarzane w postaci elektronicznej i papierowej, w szczególności dane:

- klientów i potencjalnych klientów, w tym osób korzystających z formularza kontaktowego;
- kontrahentów, dostawców, podwykonawców oraz ich pracowników i przedstawicieli;
- pracowników, współpracowników, zleceniobiorców i członków ich rodzin, gdy wymagają tego przepisy;
- kandydatów do pracy;
- osób kontaktujących się telefonicznie, e-mailowo, korespondencyjnie lub poprzez stronę internetową;
- innych osób, których dane są przetwarzane w związku z działalnością Spółki.

Zakres przetwarzanych danych, cele, podstawy prawne, kategorie osób, odbiorcy, planowane terminy usunięcia oraz ogólny opis zabezpieczeń określa Rejestr czynności przetwarzania prowadzony przez Administratora.

5. Zasady przetwarzania danych osobowych

Administrator oraz osoby upoważnione przestrzegają następujących zasad:

1. zgodność z prawem, rzetelność i przejrzystość - dane są przetwarzane na właściwej podstawie prawnej i w sposób zrozumiały dla osoby;
2. ograniczenie celu - dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach;
3. minimalizacja danych - przetwarza się wyłącznie dane adekwatne i niezbędne;
4. prawidłowość - dane są, w miarę możliwości, aktualne i poprawne;
5. ograniczenie przechowywania - dane nie są przechowywane dłużej, niż jest to konieczne;
6. integralność i poufność - dane są zabezpieczane przed utratą, zniszczeniem, zmianą i nieuprawnionym dostępem;
7. rozliczalność - Administrator dokumentuje zgodność działań z przepisami i niniejszą Polityką.

6. Role i odpowiedzialność

6.1. Administrator

- zatwierdza Politykę i zapewnia zasoby niezbędne do jej stosowania;
- ustala cele i sposoby przetwarzania danych;
- zapewnia prowadzenie wymaganej dokumentacji;
- zatwierdza poziom akceptowanego ryzyka i odpowiednie zabezpieczenia;
- zapewnia obsługę praw osób oraz naruszeń;
- weryfikuje podmioty przetwarzające i zawiera wymagane umowy;
- zapewnia szkolenia oraz kontrolę przestrzegania zasad.

6.2. Osoba koordynująca ochronę danych

Jeżeli Administrator wyznaczy osobę koordynującą ochronę danych, wspiera ona prowadzenie dokumentacji, organizację szkoleń, obsługę żądań i naruszeń oraz przeglądy zgodności. Wyznaczenie koordynatora nie przenosi odpowiedzialności Administratora.

6.3. Inspektor ochrony danych

Jeżeli powstanie prawny obowiązek wyznaczenia Inspektora Ochrony Danych albo Administrator podejmie taką decyzję dobrowolnie, jego status i zadania określa RODO. Do czasu formalnego wyznaczenia i opublikowania danych kontaktowych nie należy posługiwać się określeniem „Inspektor Ochrony Danych”.

6.4. Osoby upoważnione

- przetwarzają dane wyłącznie na polecenie Administratora i w zakresie udzielonego upoważnienia;
- zachowują dane i sposoby ich zabezpieczenia w poufności;
- stosują wymagane zabezpieczenia, w tym zasady dotyczące haseł, poczty, urządzeń i dokumentów;
- niezwłocznie zgłaszają incydenty, pomyłki i podejrzenia naruszeń;
- uczestniczą w szkoleniach i potwierdzają zapoznanie się z dokumentacją.

7. Inwentaryzacja i rejestr czynności przetwarzania

1. Administrator identyfikuje procesy, w których występują dane osobowe, i dokumentuje je w Rejestrze czynności przetwarzania.

2. Rejestr jest aktualizowany przed rozpoczęciem nowego procesu, wdrożeniem nowego systemu, pozyskaniem nowej kategorii danych, zmianą celu, odbiorców, retencji lub transferu poza EOG.

3. Za przekazanie informacji o planowanej zmianie odpowiada osoba inicjująca projekt lub zakup usługi.

4. Administrator prowadzi także wykaz podmiotów przetwarzających oraz, gdy działa jako procesor, rejestr kategorii czynności przetwarzania.

8. Podstawy prawne, obowiązek informacyjny i zgody

1. Przed rozpoczęciem przetwarzania Administrator określa cel oraz odpowiednią podstawę prawną. Zgoda nie jest stosowana, gdy właściwą podstawą jest wykonanie umowy, obowiązek prawny lub prawnie uzasadniony interes.

2. Jeżeli podstawą jest prawnie uzasadniony interes, Administrator dokumentuje cel, konieczność przetwarzania oraz ocenę wpływu na prawa i wolności osoby, gdy jest to zasadne.

3. Obowiązek informacyjny realizuje się w chwili pozyskiwania danych albo w terminach przewidzianych przez RODO, z zastosowaniem warstwowego i przejrzystego przekazu.

4. Jeśli przetwarzanie opiera się na zgodzie, zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna, a jej udzielenie oraz wycofanie należy móc wykazać. Wycofanie zgody powinno być równie łatwe jak jej udzielenie.

5. Zgody marketingowe i na komunikację elektroniczną są pozyskiwane odrębnie od akceptacji regulaminów i klauzul informacyjnych.

9. Privacy by design i privacy by default

Każdy nowy projekt, system, formularz, integracja, kampania lub zmiana procesu obejmująca dane osobowe musi zostać oceniona przed wdrożeniem. Należy w szczególności ustalić:

- cel i podstawę prawną;
- minimalny zakres danych i dostępów;
- okres przechowywania;
- odbiorców i podmioty przetwarzające;
- ryzyko dla praw i wolności osób;
- wymagane zabezpieczenia;
- sposób realizacji obowiązku informacyjnego i praw osób;
- czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych (DPIA).

10. Upoważnienia i zarządzanie dostępem

1. Dostęp do danych jest nadawany zgodnie z zasadą najmniejszych uprawnień i wyłącznie w zakresie niezbędnym do wykonywania obowiązków.

2. Przed dopuszczeniem do danych osoba otrzymuje upoważnienie, zapoznaje się z Polityką i składa zobowiązanie do poufności.

3. Administrator prowadzi ewidencję upoważnień, zawierającą co najmniej osobę, zakres, datę nadania, zmianę i cofnięcie dostępu.

4. Dostępy są przeglądane okresowo oraz niezwłocznie zmieniane lub odbierane po zmianie stanowiska, zakończeniu współpracy lub ustaniu potrzeby biznesowej.

5. Konta są indywidualne. Zabrania się współdzielenia haseł i korzystania z kont innych osób, z wyjątkiem formalnie zarządzanych kont technicznych.

11. Bezpieczeństwo danych

11.1. Zasady ogólne

Administrator dobiera środki techniczne i organizacyjne na podstawie aktualnej analizy ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania, stan wiedzy technicznej, koszty wdrożenia oraz potencjalne skutki dla osób.

11.2. Minimalne środki organizacyjne

- udokumentowane upoważnienia i zobowiązania do poufności;
- szkolenia wstępne i okresowe;
- zasada czystego biurka i czystego ekranu;
- kontrola dostępu do pomieszczeń, szaf i dokumentacji;
- bezpieczne niszczenie dokumentów i nośników;
- weryfikacja odbiorcy przed wysłaniem danych;
- procedury tworzenia kopii zapasowych, naruszeń i zakończenia współpracy;
- okresowe przeglądy zgodności i skuteczności zabezpieczeń.

11.3. Minimalne środki techniczne

- indywidualne konta użytkowników i silne, unikalne hasła;

- uwierzytelnianie wieloskładnikowe dla poczty, hostingu, panelu strony, usług chmurowych i kont administracyjnych, jeżeli usługa je umożliwia;
- regularne aktualizacje systemów, aplikacji, wtyczek i urządzeń;
- ochrona antymalware i zapora sieciowa;
- szyfrowanie transmisji oraz szyfrowanie urządzeń przenośnych, jeśli jest dostępne i adekwatne;
- automatyczna blokada ekranu i ograniczenie uprawnień administratora lokalnego;
- regularne kopie zapasowe oraz testy ich odtwarzania;
- rejestrowanie istotnych zdarzeń i monitorowanie kont administracyjnych;
- bezpieczna konfiguracja strony internetowej, formularzy i poczty;
- usuwanie lub anonimizacja danych po upływie retencji.

11.4. Poczta elektroniczna i komunikacja

- przed wysłaniem wiadomości należy zweryfikować odbiorców, adresy i załączniki;
- przy korespondencji do wielu niezależnych odbiorców stosuje się pole UDW/BCC;
- dane o podwyższonej wrażliwości lub większym zakresie przekazuje się kanałem adekwatnie zabezpieczonym;
- podejrzane wiadomości, linki i prośby o zmianę numeru rachunku wymagają niezależnej weryfikacji;
- nie wolno automatycznie przekazywać poczty służbowej na prywatne skrzynki.

11.5. Praca zdalna i urządzenia mobilne

- dane nie mogą być widoczne dla osób postronnych;
- urządzenia muszą być zabezpieczone kodem lub hasłem oraz automatyczną blokadą;
- korzystanie z publicznych sieci wymaga bezpiecznego połączenia;
- utratę urządzenia należy zgłosić niezwłocznie;
- dokumentów papierowych nie pozostawia się bez nadzoru i nie wyrzuca do zwykłych odpadów.

12. Analiza ryzyka i ocena skutków dla ochrony danych

1. Administrator prowadzi i dokumentuje analizę ryzyka dla procesów, systemów oraz zasobów wykorzystywanych do przetwarzania danych.

2. Analiza obejmuje co najmniej aktywa, zagrożenia, podatności, istniejące zabezpieczenia, prawdopodobieństwo, możliwe skutki dla osób oraz decyzję dotyczącą dalszego postępowania z ryzykiem.

3. Analizę aktualizuje się co najmniej raz w roku oraz po istotnej zmianie, incydencie, wdrożeniu systemu, zmianie dostawcy lub pojawieniu się nowego zagrożenia.

4. Jeżeli rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób, przed rozpoczęciem przetwarzania przeprowadza się DPIA. Jeżeli wysokiego ryzyka nie można ograniczyć, rozważa się uprzednie konsultacje z Prezesem UODO.

13. Powierzenie i udostępnianie danych

1. Przed powierzeniem danych Administrator weryfikuje, czy dostawca zapewnia wystarczające gwarancje zgodności i bezpieczeństwa.

2. Powierzenie następuje na podstawie umowy lub innego instrumentu prawnego spełniającego wymagania art. 28 RODO. Umowa określa m.in. przedmiot, czas, charakter, cel, rodzaj danych, kategorie osób oraz obowiązki stron.

3. Administrator prowadzi wykaz podmiotów przetwarzających, w tym hostingu, poczty, systemów IT, księgowości, kopii zapasowych i innych usługodawców mających dostęp do danych.

4. Udostępnienie danych innemu administratorowi wymaga podstawy prawnej i udokumentowania celu oraz zakresu przekazania.

5. Przekazanie danych poza Europejski Obszar Gospodarczy wymaga identyfikacji mechanizmu legalizującego transfer, oceny dostawcy i przekazania wymaganych informacji osobom, których dane dotyczą.

14. Retencja i bezpieczne usuwanie danych

1. Dane przechowuje się przez okres niezbędny do realizacji celu, obowiązku prawnego, wykonania umowy, zabezpieczenia roszczeń lub do czasu skutecznego sprzeciwu albo wycofania zgody, zależnie od podstawy przetwarzania.

2. Szczegółowe okresy retencji określa Rejestr czynności przetwarzania lub odrębny harmonogram retencji.

3. Po upływie okresu retencji dane usuwa się, anonimizuje albo archiwizuje, jeżeli obowiązek dalszego przechowywania wynika z prawa.

4. Usuwanie obejmuje systemy podstawowe, foldery współdzielone, skrzynki pocztowe i nośniki, z uwzględnieniem cyklu rotacji kopii zapasowych.

5. Dokumenty papierowe niszczy się w sposób uniemożliwiający odtworzenie danych, a nośniki elektroniczne poddaje się bezpiecznemu kasowaniu lub fizycznemu zniszczeniu.

15. Realizacja praw osób

Administrator zapewnia obsługę żądań dotyczących dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu oraz wycofania zgody.

8. Każde żądanie jest rejestrowane wraz z datą wpływu i sposobem realizacji.
9. Przed udzieleniem informacji weryfikuje się tożsamość w sposób proporcjonalny do ryzyka.
10. Odpowiedzi udziela się bez zbędnej zwłoki, zasadniczo w terminie jednego miesiąca, z możliwością przedłużenia zgodnie z RODO.
11. Żądanie przekazuje się osobie odpowiedzialnej za jego obsługę niezwłocznie po otrzymaniu.
12. Odmowa lub ograniczenie realizacji musi mieć podstawę prawną i zostać uzasadnione.

16. Naruszenia ochrony danych osobowych

1. Każda osoba mająca wiedzę lub podejrzenie naruszenia zgłasza je niezwłocznie osobie wyznaczonej przez Administratora, podając znane okoliczności, zakres danych, osoby i podjęte działania.

2. Administrator zabezpiecza dowody, ogranicza skutki, ustala przyczyny i ocenia ryzyko dla praw i wolności osób.

3. Każde naruszenie jest dokumentowane w Rejestrze naruszeń, również gdy nie podlega zgłoszeniu organowi nadzorczemu.

4. Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób, Administrator zgłasza je Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości nie później niż 72 godziny od stwierdzenia naruszenia.

5. Jeżeli naruszenie może powodować wysokie ryzyko, osoby, których dane dotyczą, są informowane bez zbędnej zwłoki, chyba że zachodzi wyjątek przewidziany w RODO.

Kanał zgłoszeń wewnętrznych
Incydenty należy zgłaszać przełożonemu lub osobie wskazanej przez Zarząd. Docelowy adres e-mail i numer telefonu do zgłoszeń należy wpisać w Procedurze obsługi naruszeń oraz zakomunikować wszystkim osobom upoważnionym.

17. Szkolenia i poufność

1. Przed dopuszczeniem do danych osoba odbywa szkolenie wstępne i potwierdza znajomość zasad ochrony danych.

2. Szkolenia okresowe odbywają się adekwatnie do ryzyka, zmian przepisów, systemów, obowiązków lub po incydentach.

3. Administrator prowadzi dokumentację szkoleń, obejmującą co najmniej datę, zakres i uczestników.

4. Obowiązek poufności trwa także po ustaniu zatrudnienia lub współpracy.

18. Kontrola, testowanie i przeglądy

1. Administrator regularnie testuje, mierzy i ocenia skuteczność środków technicznych i organizacyjnych.

2. Co najmniej raz w roku przeprowadza się przegląd Polityki, rejestrów, upoważnień, dostawców, retencji, kopii zapasowych i realizacji zaleceń z analizy ryzyka.

3. Dodatkowy przegląd przeprowadza się po poważnym incydencie, zmianie przepisów, reorganizacji, wdrożeniu nowego systemu lub zmianie istotnego dostawcy.

4. Wyniki przeglądów, wykryte niezgodności, działania korygujące, osoby odpowiedzialne i terminy są dokumentowane.

19. Postępowanie przy zakończeniu współpracy

- cofnięcie upoważnienia i dostępów nie później niż w dniu zakończenia współpracy;
- zwrot sprzętu, dokumentów, nośników, kluczy i identyfikatorów;
- zabezpieczenie lub przeniesienie służbowej poczty i plików zgodnie z prawem i zasadą minimalizacji;
- potwierdzenie usunięcia danych Spółki z prywatnych urządzeń, jeżeli ich użycie było dopuszczone;
- przypomnienie o dalszym obowiązku poufności.

20. Dokumenty powiązane

Niniejsza Polityka jest dokumentem nadrzędnym. Jej stosowanie powinno być uzupełnione co najmniej przez:

- Rejestr czynności przetwarzania;
- Analizę ryzyka i plan postępowania z ryzykiem;
- Wykaz środków technicznych i organizacyjnych;
- Procedurę obsługi naruszeń i Rejestr naruszeń;
- Procedurę realizacji praw osób i Rejestr żądań;
- Ewidencję osób upoważnionych oraz wzór upoważnienia i zobowiązania do poufności;
- Wykaz podmiotów przetwarzających i umowy powierzenia;
- Harmonogram retencji danych;

- Procedurę tworzenia i testowania kopii zapasowych;
- Procedurę nadawania, zmiany i odbierania dostępów;
- Klauzule informacyjne i rejestr stosowanych zgód, jeżeli są wykorzystywane.

21. Postanowienia końcowe

1. Polityka wchodzi w życie z dniem zatwierdzenia przez osobę uprawnioną do reprezentowania Administratora.

2. Naruszenie zasad Polityki może skutkować cofnięciem uprawnień, odpowiedzialnością pracowniczą, kontraktową albo inną przewidzianą prawem.

3. W sprawach nieuregulowanych stosuje się RODO, ustawę o ochronie danych osobowych oraz właściwe przepisy szczególne.

4. Aktualna wersja Polityki musi być dostępna dla wszystkich osób, których obowiązki obejmują przetwarzanie danych osobowych.

Załącznik A. Karta zatwierdzenia dokumentu

Nazwa	Polityka ochrony danych osobowych
Wersja	1.0
Data przyjęcia	29 września 2026 r.
Data wejścia w życie	29 września 2026 r.
Zatwierdził	_____
Podpis	_____

Załącznik B. Historia zmian

Wersja	Data	Zakres zmian	Opracował	Zatwierdził
1.0	29.09.2026	Pierwsze wydanie	_____	_____

Załącznik C. Potwierdzenie zapoznania się z Polityką

Potwierdzam, że zapoznałem(-am) się z Polityką ochrony danych osobowych WARMEKO Sp. z o.o., rozumiem wynikające z niej obowiązki i zobowiązuję się do ich przestrzegania oraz zachowania poufności danych osobowych i informacji o stosowanych zabezpieczeniach.

Imię i nazwisko	Stanowisko / rola	Data	Podpis
