MedSales Academy

https://medsales-academy.sendpulse.courses/

Zarejestrowano w Rzeczypospolitej Polskiej

POLITYKA PRZETWARZANIA DANYCH OSOBOWYCH

Wewnętrzny dokument normatywny · Zgodny z RODO i prawem Rzeczypospolitej Polskiej

---

Dokument opracowano zgodnie z: Rozporządzeniem (UE) 2016/679 (RODO); Ustawą polską z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000); Ustawą z dnia 18.07.2002 r. o świadczeniu usług drogą elektroniczną; Ustawą z dnia 16.07.2004 r. Prawo telekomunikacyjne (w zakresie cookies). Organ kontrolny: UODO (Urząd Ochrony Danych Osobowych).

1. Postanowienia ogólne i podstawa prawna

1.1. Niniejsza Polityka przetwarzania danych osobowych (dalej — „Polityka") jest wewnętrznym dokumentem normatywnym IHOR HRYTSENKO (dalej — „Administrator"), zarejestrowanego w Rzeczypospolitej Polskiej, prowadzącego działalność edukacyjną w ramach projektu MedSales Academy.

1.2. Celem Polityki jest określenie zasad, procedur i instrumentów zapewniających przetwarzanie danych osobowych zgodnie z RODO i powiązanym prawem polskim.

1.3. Polityka obowiązuje:

- — wszystkich pracowników i osoby działające w imieniu Administratora, mające dostęp do danych osobowych;
- — wszystkich podmiotów przetwarzających, z którymi Administrator zawarł DPA (umowę powierzenia przetwarzania danych, art. 28 RODO);
- — wszystkie operacje przetwarzania danych osobowych klientów, potencjalnych klientów i partnerów.

1.4. Administrator wyznacza osobę odpowiedzialną za ochronę danych (IOD — jeżeli ma zastosowanie art. 37 RODO) lub osobę odpowiedzialną za wypełnianie obowiązków w zakresie ochrony danych.

2. Rejestr czynności przetwarzania (RoPA — art. 30 RODO)

2.1. Administrator prowadzi pisemny rejestr wszystkich czynności przetwarzania danych osobowych (Record of Processing Activities) zgodnie z art. 30 RODO, zawierający:

1. nazwę i dane kontaktowe Administratora oraz, w stosownych przypadkach, IOD;

2. cele przetwarzania;

3. kategorie osób, których dane dotyczą, oraz kategorie danych osobowych;

4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;

5. informacje o przekazywaniu do państw trzecich i zastosowanych zabezpieczeniach;

6. przewidywane terminy usunięcia poszczególnych kategorii danych;

7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 RODO).

2.2. RoPA jest aktualizowany przy każdej zmianie operacji przetwarzania i udostępniany na żądanie UODO.

3. Kategorie danych osobowych i podmiotów danych

Baza danych	Kategorie podmiotów	Kategorie danych
Klienci i użytkownicy	Osoby fizyczne — kupujący kurs	Imię, nazwisko, e-mail, telefon, dane płatnicze, postęp nauki, IP
Potencjalni klienci	Osoby, które złożyły zapytanie	Imię, e-mail, telefon, treść zapytania
Pracownicy	Personel Administratora	Zgodnie z polskim prawem pracy (odrębny regulamin)
Marketing (za zgodą)	Subskrybenci newslettera	E-mail, imię, data/sposób wyrażenia zgody

3.1. Administrator NIE przetwarza szczególnych kategorii danych (art. 9 RODO) bez wyraźnej i odrębnej zgody osoby, której dane dotyczą, lub bez innej podstawy przewidzianej w art. 9(2) RODO.

3.2. Dane osobowe dzieci poniżej 16 roku życia (zgodnie z art. 8 RODO i art. 5 polskiej Ustawy z dnia 10.05.2018 r.) mogą być przetwarzane wyłącznie za zgodą rodziców lub opiekunów prawnych. Usługi MedSales Academy są przeznaczone wyłącznie dla osób, które ukończyły 18 lat.

4. Zasady przetwarzania danych osobowych (art. 5 RODO)

4.1. Wszelkie operacje przetwarzania danych osobowych są realizowane zgodnie z następującymi zasadami:

1. Zgodność z prawem, rzetelność i przejrzystość (art. 5(1)(a)) — przetwarzanie wyłącznie na zgodnych z prawem podstawach i w sposób zrozumiały dla osoby, której dane dotyczą.
2. Ograniczenie celu (art. 5(1)(b)) — zbieranie wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach; dalsze przetwarzanie niezgodne z pierwotnym celem jest niedopuszczalne.
3. Minimalizacja danych (art. 5(1)(c)) — przetwarzane są wyłącznie dane adekwatne, stosowne i niezbędne.
4. Prawidłowość (art. 5(1)(d)) — dane są utrzymywane w aktualności; nieprawidłowe — niezwłocznie poprawiane lub usuwane.
5. Ograniczenie przechowywania (art. 5(1)(e)) — dane są przechowywane w formie umożliwiającej identyfikację nie dłużej, niż jest to niezbędne dla celów przetwarzania.

6. Integralność i poufność (art. 5(1)(f)) — ochrona przed niedozwolonym przetwarzaniem, utratą lub zniszczeniem.

7. Rozliczalność (art. 5(2)) — Administrator jest w stanie wykazać przestrzeganie wszystkich zasad.

5. Podstawy prawne przetwarzania (art. 6 RODO) — szczegółowe omówienie

5.1. Przetwarzanie na podstawie zgody (art. 6(1)(a) RODO):

— Zgoda jest uzyskiwana w formie wyraźnego działania twierdzącego (opt-in): pole wyboru w formularzu rejestracyjnym, potwierdzenie w e-mailu.

— Każdy cel — odrębna zgoda (marketing nie jest łączony z warunkami usługi).

— Administrator dokumentuje: przez kogo, kiedy, w jaki sposób i w jakim celu zgoda została udzielona.

— Cofnięcie następuje: poprzez ustawienia konta, link w wiadomości e-mail, wniosek e-mailowy. Cofnięcie nie wpływa na zgodność z prawem przetwarzania przed cofnięciem.

5.2. Przetwarzanie w celu wykonania umowy (art. 6(1)(b) RODO):

— Podstawą jest umowa z osobą, której dane dotyczą, lub działania na jej wniosek przed zawarciem umowy.

— Podanie danych jest warunkiem koniecznym świadczenia usługi; bez nich wykonanie umowy jest niemożliwe.

5.3. Przetwarzanie w celu wypełnienia obowiązku prawnego (art. 6(1)(c) RODO):

— Prowadzenie dokumentacji finansowej (Ustawa polska z dnia 29.09.1994 r. o rachunkowości).

— Wypełnienie wymogów prawa podatkowego (Ustawa o VAT, Ustawa o podatku dochodowym).

— Udostępnienie danych uprawnionym organom na zgodnych z prawem podstawach.

5.4. Przetwarzanie na podstawie uzasadnionego interesu (art. 6(1)(f) RODO):

— Ochrona Administratora przed oszustwami i naruszeniami warunków korzystania.

— Analityka i poprawa jakości usług (zanonimizowane statystyki).

— Ochrona praw w sporach sądowych i pozasądowych.

— Administrator przeprowadza udokumentowany test równowagi interesów dla każdego celu opartego na tej podstawie.

6. Zarządzanie zgodami i ich cofaniem

6.1. Wymagania dotyczące ważnej zgody (art. 7 RODO):

— Dobrowolna — nie może być uzależniona od świadczenia usługi (z wyjątkiem przypadków, gdy przetwarzanie jest niezbędne do jej wykonania).

— Konkretna — dla każdego celu odrębnie.

— Świadoma — jasny opis celu, kategorii danych, prawa do cofnięcia zgody.

— Jednoznaczna — wyrażona przez działanie twierdzące (nie wstępnie zaznaczone pola, nie milczenie).

6.2. Administrator prowadzi rejestr udzielonych/cofniętych zgód z podaniem: ID osoby, daty i sposobu udzielenia, dokładnej treści wyświetlonej w momencie udzielenia zgody oraz daty cofnięcia (jeśli dotyczy).

6.3. Zgoda na komunikację marketingową jest potwierdzana mechanizmem double opt-in (e-mail potwierdzający subskrypcję).

6.4. Osoba może cofnąć każdą zgodę w dowolnym momencie bez negatywnych konsekwencji dla dostępu do usług, które nie zależą od tej zgody.

7. Okresy przechowywania danych osobowych

Kategoria danych	Okres przechowywania	Podstawa prawna
Dane umowne klientów	5 lat od zakończenia umowy	art. 6(1)(b)(c) RODO + Ustawa o rachunkowości PL
Dokumenty płatnicze i fiskalne	5 lat od końca roku obrotowego	Prawo podatkowe PL
Zgody marketingowe	Do cofnięcia + 3 lata na dowody	art. 6(1)(a) RODO
Logi techniczne / bezpieczeństwo	12 miesięcy	art. 6(1)(f) RODO
Zapytania do wsparcia	2 lata po zamknięciu	art. 6(1)(f) RODO
Nieaktywne konta	3 lata od ostatniej aktywności	art. 6(1)(f) RODO
Analityczne pliki cookie	13 miesięcy	Zalecenia UODO / CNIL
Dane o naruszeniach bezpieczeństwa	5 lat (dokumentacja)	art. 33(5) RODO

7.1. Po upływie okresu przechowywania dane osobowe są niszczone w bezpieczny sposób lub anonimizowane. Procedura niszczenia jest dokumentowana.

8. Ocena skutków dla ochrony danych (DPIA — art. 35 RODO)

8.1. Administrator przeprowadza DPIA przed rozpoczęciem operacji przetwarzania, które mogą powodować wysokie ryzyko dla praw i wolności osób fizycznych, w szczególności:

— systematyczne i zakrojone na szeroką skalę profilowanie;

— przetwarzanie szczególnych kategorii danych na dużą skalę;

— systematyczne monitorowanie miejsc publicznie dostępnych na dużą skalę.

8.2. Jeżeli DPIA wskazuje na wysokie ryzyko szczątkowe, Administrator zwraca się do UODO o uprzednią konsultację (art. 36 RODO).

9. Podmioty przetwarzające i strony trzecie (art. 28–29 RODO)

9.1. Przed zaangażowaniem podmiotu przetwarzającego Administrator przeprowadza weryfikację:

— istnienia technicznych i organizacyjnych środków zgodnych z RODO;

— przestrzegania zasad ochrony danych i rozliczalności;

— jurysdykcji i odpowiednich mechanizmów przekazania do państw trzecich.

9.2. Z każdym podmiotem przetwarzającym zawierana jest DPA (umowa powierzenia przetwarzania danych) zawierająca obowiązkowe elementy art. 28(3) RODO: przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych, kategorie osób, prawa i obowiązki stron.

9.3. Podmiot przetwarzający może angażować dalsze podmioty przetwarzające wyłącznie za uprzednią pisemną zgodą Administratora. Administrator prowadzi aktualną listę podmiotów przetwarzających i dalszych podmiotów przetwarzających.

9.4. Dalsze podmioty przetwarzające są zobowiązane spełniać te same wymagania w zakresie ochrony danych co główny podmiot przetwarzający.

10. Techniczne i organizacyjne środki ochrony (art. 32 RODO)

10.1. Środki techniczne (z uwzględnieniem „stanu wiedzy technicznej" zgodnie z art. 32(1)):

— Szyfrowanie podczas transmisji (TLS 1.2+) i w stanie spoczynku (AES-256 lub odpowiednik).

— Pseudonimizacja danych osobowych (gdzie jest technicznie wykonalna).

— Tworzenie kopii zapasowych z weryfikacją przywracania.

— Logowanie dostępu do danych osobowych.

— Zarządzanie podatnościami i regularne aktualizacje oprogramowania.

— Uwierzytelnianie wieloskładnikowe dla systemów administracyjnych.

10.2. Środki organizacyjne:

— Wyznaczenie osób odpowiedzialnych za poszczególne kategorie przetwarzania.

— Regularne szkolenia personelu (nie rzadziej niż raz w roku) z zakresu RODO i cyberbezpieczeństwa.

— Jasne wewnętrzne procedury obsługi wniosków osób, których dane dotyczą.

— Procedura reagowania na naruszenia bezpieczeństwa z checklistą i terminami.

— Weryfikacja stron trzecich (due diligence) przed zawarciem DPA.

— Regularne wewnętrzne audyty zgodności z RODO (nie rzadziej niż raz w roku).

11. Procedura reagowania na naruszenia bezpieczeństwa (art. 33–34 RODO)

11.1. Po stwierdzeniu lub podejrzeniu naruszenia ochrony danych osobowych osoba odpowiedzialna jest zobowiązana:

1. Niezwłocznie odnotować fakt stwierdzenia z dokładnym czasem.

2. Przeprowadzić wstępną ocenę ryzyka dla praw i wolności osób, których dane dotyczą, w ciągu 1 (jednej) godziny.

3. Jeżeli ryzyko nie jest nieznaczne — zgłosić naruszenie do UODO w ciągu 72 (siedemdziesięciu dwóch) godzin od stwierdzenia (art. 33(1) RODO). Jeżeli zgłoszenie jest opóźnione — podać przyczyny.

4. Jeżeli ryzyko jest „wysokie" — bez zbędnej zwłoki powiadomić bezpośrednio poszkodowane osoby (art. 34 RODO).

5. Udokumentować incydent w rejestrze naruszeń z: opisem naruszenia, kategoriami i liczbą poszkodowanych osób, możliwymi konsekwencjami, podjętymi działaniami.
6. Przeprowadzić analizę po incydentową i wdrożyć środki prewencyjne.

11.2. Zgłoszenie do UODO (art. 33(3) RODO) zawiera: charakter naruszenia, kategorie i przybliżoną liczbę poszkodowanych, dane kontaktowe IOD, prawdopodobne konsekwencje, podjęte lub planowane środki.

12. Prawa osób i wewnętrzna procedura ich realizacji

12.1. Wniosek osoby może wpłynąć w dowolnej formie (e-mail, poczta, ustnie). Osoba odpowiedzialna rejestruje wniosek niezwłocznie po jego otrzymaniu.

12.2. Terminy odpowiedzi: 1 (jeden) miesiąc od daty otrzymania wniosku. W przypadku skomplikowanych wniosków — przedłużenie o 2 (dwa) miesiące z powiadomieniem w pierwszym miesiącu.

12.3. Weryfikacja tożsamości osoby jest przeprowadzana środkami proporcjonalnymi do ryzyka błędnej identyfikacji (bez nadmiernego zbierania dodatkowych danych).

12.4. Jeżeli wniosek jest ewidentnie nieuzasadniony lub nadmierny (np. powtarzający się), Administrator może odmówić jego realizacji lub pobrać uzasadnioną opłatę, dokumentując decyzję.

12.5. Rejestr wniosków osób jest przechowywany na potrzeby wykazania rozliczalności (art. 5(2) RODO).

13. Szkolenia i podnoszenie świadomości

13.1. Wszystkie osoby mające dostęp do danych osobowych przechodzą obowiązkowe szkolenie wstępne z zakresu RODO przed rozpoczęciem przetwarzania oraz coroczne szkolenie uzupełniające.

13.2. Program szkolenia obejmuje: zasady RODO, podstawy prawne, prawa osób, procedurę reagowania na naruszenia, bezpieczne praktyki przetwarzania.

13.3. Fakt odbycia szkolenia jest dokumentowany.

14. Zmiany Polityki i przegląd

14.1. Niniejsza Polityka jest przeglądana nie rzadziej niż raz w roku, a także w przypadku: istotnych zmian w przepisach prawa lub zaleceniach UODO; wprowadzenia nowych operacji przetwarzania; stwierdzonych naruszeń lub wyników audytu.

14.2. Wszystkie wersje Polityki są archiwizowane przez co najmniej 5 (pięć) lat.

15. Dane kontaktowe

Administrator: IHOR HRYTSENKO

Adres: Region Śląskie, Gliwice, ul. Czwartaków 11/27, Polska

NIP: 6312731797 / REGON: Śląskie

E-mail: medsales.academyonline@gmail.com

Niniejsza Polityka została zatwierdzona przez Administratora i wchodzi w życie z dniem podpisania.