+48 720 177 174
+48 511 019 652
contact@airtilion.com
Airtilion Sp. z o.o.
NIP: 8733299720
REGON: 540390460000000
KRS: 0001143482

POLITYKA OCHRONY DANYCH OSOBOWYCH - Airtilion Sp. z o.o.

1. Cel i zakres polityki

Polityka określa cele oraz organizacyjne i techniczne środki ochrony danych osobowych przetwarzanych przez Airtilion (klienci, kontrahenci, pracownicy), w celu zapewnienia zgodności z RODO i krajowymi przepisami.

2. Administrator danych

Airtilion Sp. z o.o., ul. Słoneczna 32/9, 33-100 Tarnów. Kontakt w sprawach ochrony danych: contact@airtilion.com.

3. Rejestr czynności przetwarzania

Airtilion prowadzi rejestr czynności przetwarzania obejmujący m.in.: kontakt z klientami (formularz/email/telefon), realizacja umów, fakturowanie, marketing (zgody), rekrutacja (jeśli występuje), backupy i logi serwera. Rejestr zawiera cele, okresy przechowywania, kategorie odbiorców, podstawy prawne.

4. Podstawy prawne przetwarzania

Wymienienie podstaw: art. 6 RODO (zgoda - a; realizacja umowy - b; obowiązek prawny - c; prawnie uzasadniony interes - f). Szczegółowe przydzielenie podstaw do poszczególnych czynności (np. wysyłka oferty - zgoda lub uzasadniony interes, odpowiadanie na zapytanie z formularza - uzasadniony interes).

5. Kategorie danych i okresy przechowywania

- Dane kontaktowe klientów: e-mail, telefon, imię - przechowywane do czasu cofnięcia zgody lub zakończenia okresu rozliczeniowego/archiwalnego zgodnie z polityką retencji (zwykle 5 lat dla celów księgowych/podatkowych, dokumenty księgowe dłużej - zgodnie z przepisami).
- Dane w korespondencji: przechowywane do czasu usunięcia przez klienta lub do momentu przedawnienia roszczeń/archiwizacji.
  (Ustal szczegóły okresów w tabeli retencji).

6. Upoważnienia i dostęp

- Upoważnienia do przetwarzania danych wydawane są na piśmie/elektronicznie, ewidencjonowane i okresowo weryfikowane.
- Dostęp do danych w systemach ograniczony jest rolami (RBAC). Hasła muszą spełniać politykę haseł; konta użytkowników likwidowane przy zmianie zatrudnienia.

7. Środki techniczne

Przykładowe środki (dostosuj do środowiska):

- Szyfrowanie komunikacji TLS 1.2/1.3 na serwerach i stronach.
- Szyfrowanie kopii zapasowych i nośników przenośnych (AES-256).
- Regularne backupy (dziennie/tygodniowo) przechowywane w chmurze z redundancją.
- Aktualizacje systemów i aplikacji według polityki patchowania (co najmniej raz w miesiącu).
- Monitorowanie logów i systemów (IDS/monitoring dostępów).
- Ograniczenie dostępu do środowisk produkcyjnych (VPN, 2FA dla administratorów).

8. Środki organizacyjne

- Regularne szkolenia pracowników z zakresu ochrony danych (co najmniej raz w roku).
- Procedura obsługi naruszeń ochrony danych (zgłaszanie do Prezesa UODO w ciągu 72 godzin, dokumentacja incydentu).
- Procedury tworzenia kopii zapasowych, testów odtwarzania i testów bezpieczeństwa.
- Procedury usuwania danych po zakończeniu retencji.

9. Powierzenia przetwarzania (subprocesory)

- Wzór umowy powierzenia przetwarzania danych (DPA) : musi zawierać cel, zakres, obowiązki powiernika, środki ochrony, audyt i zasady zwrotu/usunięcia danych.
- Lista aktualnych powierników (np. dostawca hostingu, dostawca chmury, dostawca narzędzi mailingowych, księgowość) powinna być utrzymywana i aktualizowana.

10. Transfery poza EOG

- W przypadku transferu danych poza Europejski Obszar Gospodarczy - stosujemy mechanizmy prawne (standardowe klauzule umowne, decyzje adequacy, itp.) i dokumentujemy podstawę prawną. (Jeśli korzystasz z Google/Meta - zdecyduj i udokumentuj podstawy).

11. Realizacja praw osób, których dane dotyczą

- Procedury obsługi żądań: dostęp, sprostowanie, usunięcie, ograniczenie, przenoszenie, sprzeciw, cofnięcie zgody. Czas odpowiedzi: max. 1 miesiąc, z możliwością przedłużenia w uzasadnionych przypadkach.

12. Naruszenia ochrony danych

- Procedura: identyfikacja -> zawiadomienie IOD/zarządu -> ocena ryzyka -> powiadomienie Prezesa UODO w ciągu 72h (jeśli dotyczy) -> powiadomienie osób, których dane dotyczą (jeśli ryzyko wysokie). Dokumentuje się każde naruszenie w rejestrze naruszeń.

13. Audyt, nadzór i przegląd

- Politykę przegląda się rocznie lub po istotnych zmianach technicznych/prawnych. Przeprowadza się testy penetracyjne i audyt zgodności.