Polityka prywatności (RODO) – MelonManager (web + iOS/Android)

wersja: 1.2 | obowiązuje od: 4 listopada 2025 r.

1) Kim jesteśmy i czego dotyczy ten dokument

Podmiot przetwarzający („my", „MelonManager"): Targetly Krzysztof Szymczak, ul. Krótka 5, 55-040 Królikowice, NIP 896-15-69-142, REGON 368465811, e-mail: info@targetly.io.
Zakres: niniejsza Polityka dotyczy przetwarzania danych osobowych w związku z korzystaniem z aplikacji webowej pod adresem app.melonmanager.pl oraz aplikacji mobilnych na systemy iOS i Android (łącznie: „Aplikacja").
Charakter przetwarzania: działamy jako podmiot przetwarzający w imieniu naszych klientów – firm oferujących usługi/zajęcia (administratorów). Dokument nie zastępuje informacji, które administrator ma obowiązek przekazać osobom, których dane dotyczą (art. 13–14 RODO).

2) Role i odpowiedzialności

Administrator danych: każdorazowo klient MelonManager (Usługobiorca) – organizator zajęć. To administrator decyduje o celach i podstawach prawnych przetwarzania.
MelonManager jako procesor: przetwarzamy dane wyłącznie na udokumentowane polecenie administratora i na podstawie umowy powierzenia (art. 28 RODO).

3) Kategorie osób i danych

Osoby: klienci/uczestnicy usług administratora oraz użytkownicy upoważnieni administratora (np. trenerzy/recepcja).
Dane: identyfikacyjne i kontaktowe; dane kont/dostępów; dane operacyjne (zapisy/obecności/harmonogramy/komunikacja/statusy płatności, jeśli włączone);
dane techniczne: logi, identyfikatory sesji, adres IP, identyfikatory urządzeń mobilnych niezbędne do działania Aplikacji (np. push tokeny), pamięć lokalna (LocalStorage/Keychain/Keystore).
Dane szczególnych kategorii co do zasady nie są wymagane; jeśli administrator je przetwarza, czyni to we własnym zakresie.

4) Cele (po stronie administratora) i operacje (po stronie procesora)

Cele określa administrator (obsługa zapisów, relacji z klientami, rozliczeń, komunikacji, analityki, obowiązków prawnych).
Nasze operacje jako procesora: hostowanie i przechowywanie, udostępnianie funkcji zapisów/komunikacji, wysyłka komunikatów (w tym e-mail i push), kopie zapasowe i przywracanie, monitoring działania, wsparcie techniczne, testy bezpieczeństwa – zgodnie z poleceniami administratora.

5) Podstawy prawne

Podstawy wobec osób, których dane dotyczą, ustala administrator (np. art. 6 ust. 1 lit. b/f/a RODO).
Dla nas podstawą przetwarzania jest umowa powierzenia (art. 28 RODO).

6) Podprocesorzy i udostępnianie danych

Korzystamy z podprocesorów (kategorie): hosting/chmura, e-mail, powiadomienia push (APNs/FCM), monitoring/backup, wsparcie serwisowe. Każdorazowo na podstawie umów spełniających art. 28 RODO.
Utrzymujemy wykaz kategorii podprocesorów i udostępniamy go administratorom w Aplikacji lub na żądanie.
Dane nie są sprzedawane i nie są ujawniane innym odbiorcom bez polecenia administratora lub podstawy prawnej.

7) Przekazywanie danych poza EOG

Co do zasady przetwarzamy dane w EOG. W przypadku korzystania z usług powiadomień push (APNs/FCM) lub innych dostawców spoza EOG może dojść do przekazania danych poza EOG. Zapewniamy mechanizmy z rozdz. V RODO (np. standardowe klauzule umowne).

8) Retencja i usuwanie

Działamy zgodnie z instrukcjami retencji administratora i art. 28 ust. 3 lit. g RODO (zwrot/usunięcie po zakończeniu usługi).
Automatyczne usuwanie kont klientów administratora: konta użytkowników (klientów administratora) są usuwane po 12 miesiącach braku aktywności, tj. braku zapisania się na jakiekolwiek zajęcia przez rok, chyba że administrator zadecyduje inaczej.
Kopie zapasowe/logi techniczne: utrzymywane tylko tak długo, jak to konieczne do bezpieczeństwa i ciągłości działania oraz zgodnie z poleceniami administratora; po upływie tych okresów nadpisywane/usuwane.

9) Prawa osób, których dane dotyczą

Prawa: dostęp, sprostowanie, usunięcie, ograniczenie, przenoszenie, sprzeciw oraz skarga do PUODO.
Żądania należy kierować do administratora (organizatora zajęć). Jako procesor wspieramy administratora w realizacji praw (art. 28 ust. 3 lit. e RODO).
Gdy nie wiesz, kto jest administratorem, napisz do nas: info@targetly.io.

10) Bezpieczeństwo

Stosujemy adekwatne środki techniczne i organizacyjne (TLS, kontrola dostępu, minimalizacja, bezpieczne przechowywanie haseł, kopie zapasowe, rejestrowanie zdarzeń, przeglądy uprawnień, poufność personelu).

11) Naruszenia

Niezwłocznie informujemy administratora o naruszeniach i przekazujemy dane potrzebne do wypełnienia art. 33–34 RODO.

12) Cookies, identyfikatory urządzeń i SDK (web + mobile)

Web: używamy niezbędnych cookies/LocalStorage dla logowania, utrzymania sesji, bezpieczeństwa oraz analityki
Mobile (iOS/Android): aplikacje mogą używać lokalnych magazynów systemowych (np. Keychain/Keystore), push tokenów, SDK niezbędnych do działania (np. do powiadomień i stabilności) jak i tokenów do analityki zapewniającej stabilność
Narzędzia marketingowe (w tym ewentualne identyfikatory reklamowe) są aktywowane wyłącznie na polecenie administratora, który zapewnia podstawę prawną i spełnia obowiązki informacyjne.

13) Uprawnienia w urządzeniu (mobile)

W aplikacjach mobilnych możesz wyrazić/wycofać zgody systemowe (np. powiadomienia). Niektóre funkcje mogą wymagać uprawnień (np. zapis do kalendarza). Odmowa może ograniczyć funkcjonalność, ale nie wpływa na korzystanie z pozostałych funkcji.

14) Kontakt i zmiany

Podmiot przetwarzający: Targetly Krzysztof Szymczak, ul. Krótka 5, 55-040 Królikowice, info@targetly.io.
Zmiany Polityki będą ogłaszane w Aplikacji i/lub drogą elektroniczną.