Polityka Prywatności Usługi GymBox by Piko24

Definicje:

1. **Administrator** – podmiot wskazany w § 1 Polityki,
2. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **Incydent** - zdarzenie skutkujące przypadkowym lub niezgodnym z prawem ujawnieniem, zniszczeniem, utratą, zmianą lub nieuprawnionym dostępem do danych osobowych,
4. **PKE** - ustawa z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221),
5. **Użytkownik** - osoba fizyczna, której dane osobowe są przetwarzane przez Administratora,
6. **Polityka** – niniejszy dokument określający zasady przetwarzania i ochrony danych osobowych w ramach działalności Administratora, sporządzony zgodnie z obowiązującymi przepisami prawa, w szczególności Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), ustawą PKE,
7. **Regulamin** – Regulamin Usługi GymBox by Piko24,
8. **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. dotyczące ochrony osób fizycznych w kontekście przetwarzania danych osobowych oraz swobodnego przepływu tych danych, uchylające dyrektywę 95/46/WE,
9. **Zgoda użytkownika** - dobrowolne, świadome i jednoznaczne wyrażenie woli użytkownika, na mocy którego wyraża on zgodę na przetwarzanie swoich danych osobowych, w tym ewentualnie na cele marketingowe oraz stosowanie technologii śledzących.

§1. Administrator danych

1. Administratorem danych osobowych Użytkowników korzystających z usługi GymBox by Piko24 jest spółka Piko24 Sp. z o.o. z siedzibą w Mikołowie (43 – 190), ul. Rynek 2, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Katowice-Wschód w Katowicach, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0001119063, NIP: 6351871858, REGON: 529292987.
2. Dane kontaktowe Administratora:
   Telefon: +48 800 802 801
   E-mail: office@gymbox.pl
   Adres korespondencyjny: ul. Rynek 2, 43-190 Mikołów
3. W sprawach dotyczących ochrony danych osobowych można kontaktować się również przez e-mail: office@gymbox.pl
4. Spółka nie powołała Inspektora Ochrony Danych.

§2. Cele i podstawy prawne przetwarzania danych

1. Podanie danych osobowych jest dobrowolne, jednak konieczne do korzystania z usługi GymBox.

2. Dane są gromadzone przez Administratora za pomocą aplikacji GymBox służącej do realizacji Usługi GymBox, w tym zapisywane w plikach cookies, tokenach, w ramach prowadzonej komunikacji e-mailowej, sms oraz telefonicznej, a także na serwerach Administratora służących obsłudze monitoringu audiowizualnego. Rozpoczęcie korzystania z Usługi GymBox jest równoznaczne z wyrażeniem zgody przez Użytkownika na przetwarzanie, w tym gromadzenie i przechowywanie Danych w zakresie określonym w § 3.
3. Dane osobowe są przetwarzane w celu:

1. świadczenia usług związanych z korzystaniem z siłowni GymBox, w tym rezerwacji i opłacania sesji treningowych – art. 6 ust. 1 lit. b RODO (niezbędne do wykonania umowy),
2. umożliwienia logowania do aplikacji i obsługi konta użytkownika – art. 6 ust. 1 lit. b RODO (niezbędne do wykonania umowy),
3. zapewnienia bezpieczeństwa w obiekcie poprzez monitoring wideo i audio – art. 6 ust. 1 lit. f RODO (uzasadniony interes Administratora),
4. rozliczania płatności i obsługi ewentualnych reklamacji – art. 6 ust. 1 lit. b RODO (niezbędne do wykonania umowy),
5. kontaktu z użytkownikiem (telefonicznie lub mailowo) w sprawach technicznych lub dotyczących rezerwacji – art. 6 ust. 1 lit. b RODO (niezbędne do wykonania umowy),
6. realizacji obowiązków prawnych (np. rachunkowych, podatkowych) – art. 6 ust. 1 lit. c RODO,
7. poprawy jakości usług i rozwoju technologii GymBox – art. 6 ust. 1 lit. f RODO,
8. przesyłania treści informacyjnych lub promocyjnych – wyłącznie po wyrażeniu zgody użytkownika.

4. Działania marketingowe, o których mowa w ust. 3 pkt 8, mogą polegać na kierowaniu do Użytkownika informacji handlowych, po wyrażeniu przez Użytkownika zgody w tym zakresie. Zgoda taka może być wycofana w każdym momencie o czym należy poinformować Administratora.
9. Dane osobowe Użytkownika mogą zostać wykorzystane przez Administratora w celu stworzenia profilu Użytkownika w sposób automatyczny. Dane te są wykorzystywane do tworzenia spersonalizowanej oferty promocyjnej lub akcji informacyjnej dla danego Użytkownika. Administrator działa na podstawie art. 6 ust. 1 lit. f) RODO. Użytkownik może w każdej chwili sprzeciwić się profilowaniu, o czym należy poinformować Administratora.

§3. Zakres przetwarzanych danych

Administrator przetwarza dane osobowe w zakresie niezbędnym do korzystania z aplikacji i siłowni GymBox, w szczególności:

- imię i nazwisko,
- adres e-mail,
- numer telefonu,
- dane logowania do aplikacji,

- dane płatnicze (token karty, cztery ostatnie cyfry, data ważności),
- dane dotyczące aktywności w aplikacji (historia rezerwacji, liczba wejść, statystyki treningów),
- dobrowolnie podane informacje o wadze, wzroście i celach treningowych,
- wizerunek i głos (zarejestrowane w ramach systemu bezpieczeństwa w obiekcie).

§4. Specyfika przetwarzania danych

1. Dane Użytkowników są przetwarzane w aplikacji GymBox oraz na serwerach Administratora w celu obsługi konta, rezerwacji i płatności.
2. System monitoringu wideo i audio działa wyłącznie w godzinach aktywności siłowni GymBox i służy zapewnieniu bezpieczeństwa oraz ochronie mienia.
3. Dane dotyczące karty płatniczej są tokenizowane – Administrator nie przechowuje pełnych danych kart. Administrator przechowuje ostatnie cztery cyfry numeru karty płatniczej Użytkownika w celu identyfikacji Użytkownika oraz dla zapewnienia bezpieczeństwa świadczonych przez Administratora usług. Administrator przekształca w czasie rzeczywistym dane karty płatniczej Użytkownika obejmujące numer tej karty, w unikalny token, który służy do identyfikacji karty płatniczej Uczestnika, Płatności realizuje operator PayU S.A. z siedzibą w Poznaniu.
4. Dane dotyczące aktywności (np. liczba treningów, czas sesji) mogą być analizowane w celu poprawy jakości usług lub dopasowania treści aplikacji do Użytkownika.

§5. Okres przechowywania danych

1. Dane są przechowywane tylko przez okres niezbędny do realizacji celów przetwarzania, a po tym czasie są usuwane lub archiwizowane zgodnie z obowiązującymi przepisami prawa. Dane osobowe będą przechowywane w szczególności:
   a. przez okres korzystania z usługi, a po zamknięciu konta Administrator będzie przechowywać dane rozliczeniowe przez 5 lat następujących po roku, w którym wystąpił obowiązek podatkowy;
   b. do czasu wycofania zgody lub do czasu załatwienia sprawy, a następnie do upływu okresu przedawnienia roszczeń stron związanych z jej realizacją;
   c. w przypadku reklamacji, do czasu przedawnienia ewentualnych roszczeń;
   d. związane z analizą ruchu sieciowego gromadzone za pośrednictwem plików cookies oraz podobnych technologii mogą być przechowywane do momentu wygaśnięcia pliku. Niektóre pliki tego rodzaju nigdy nie wygasają, w związku z tym czas przechowywania danych będzie równoważny z czasem niezbędnym Administratorowi do zrealizowania celów związanych z gromadzeniem danych, jak zapewnienie bezpieczeństwa i analiza danych historycznych związanych z ruchem na stronie.
2. Administrator stosuje procedury regularnej weryfikacji danych, aby ograniczyć ich przechowywanie do niezbędnego minimum. Po upływie ustalonego okresu dane są usuwane lub archiwizowane.

3. Dane dotyczące komunikacji elektronicznej, w tym dane ruchu i metadane, są przechowywane zgodnie z wymogami PKE i tylko w sytuacjach niezbędnych do realizacji celów określonych przepisami prawa.

§6. Uprawnienia użytkownika

1. Użytkownikowi przysługują następujące uprawnienia w związku z przetwarzaniem danych osobowych:
   1) prawo do uzyskania informacji o celach, podstawach prawnych, zakresie przetwarzanych danych, odbiorcach oraz okresie przechowywania danych,
   2) prawo do otrzymania kopii przetwarzanych danych osobowych,
   3) prawo do poprawienia lub uzupełnienia nieścisłych lub niekompletnych danych osobowych,
   4) prawo do usunięcia lub anonimizacji danych, które nie są już potrzebne do realizacji celów, dla których zostały zebrane,
   5) prawo do żądania wstrzymania przetwarzania danych, z wyjątkiem sytuacji, gdy dane muszą być przechowywane zgodnie z polityką retencji lub na podstawie decyzji organu nadzorczego,
   6) prawo do otrzymania danych osobowych w powszechnie używanym formacie umożliwiającym ich przeniesienie do innego administratora,
   7) prawo do sprzeciwu przetwarzania jego danych w celach marketingowych,
   8) prawo do sprzeciwu wobec przetwarzania danych na podstawie prawnie uzasadnionego interesu Administratora, jeśli istnieją szczególne okoliczności,
   9) prawo do wycofania zgody na przetwarzanie danych w każdej chwili, bez wpływu na zgodność z prawem przetwarzania przed jej wycofaniem.
2. W celu realizacji uprawnień wymienionych w ust. 1, Użytkownik może skontaktować się z Administratorem, którego dane kontaktowe wskazano w § 1 ust. 2 i 3. Użytkownik może również wnieść skargę do organu nadzorczego, którym w Rzeczpospolitej Polskiej jest Prezes Urzędu Ochrony Danych Osobowych.

§7. Odbiorcy danych

1. Dane osobowe mogą być udostępniane innym podmiotom tylko wtedy, gdy spełnione są wymogi RODO. Administrator dokładnie sprawdza podstawy prawne przed udostępnieniem danych.
2. Powierzanie przetwarzania danych osobowych odbywa się na podstawie umowy powierzenia, zgodnie z art. 28 RODO, określającej cel, zakres przetwarzania oraz odpowiednie środki ochrony danych.
3. Przed powierzeniem przetwarzania danych, Administrator weryfikuje, czy podmiot przetwarzający spełnia wymagania bezpieczeństwa i stosuje odpowiednie środki ochrony danych, zapewniając zgodność z RODO.
4. Dane osobowe mogą być udostępniane:

- operatorowi technicznemu systemu – ShopBox Sp. z o.o.,
- dostawcom usług IT i hostingu,
- operatorom płatności – PayU S.A.,
- podmiotom obsługującym księgowość, prawo i marketing,
- organom publicznym uprawnionym do przetwarzania danych (np. sądy, urzędy skarbowe).

§8. Przekazywanie danych poza EOG

1. Poziom ochrony danych osobowych poza Europejskim Obszarem Gospodarczym (EOG), tj. krajami Unii Europejskiej oraz Norwegią, Liechtensteinem i Islandią jest inny od tego zapewnianego przez prawo unijne. W związku z tym Administrator nie przekazuje danych poza EOG. Nie można wykluczyć sytuacji, kiedy jest to konieczne i dochodzi do takiego transferu danych. Administrator zobowiązany jest wówczas zapewnić odpowiedni stopień ochrony, w szczególności poprzez:
   1) współpracę z podmiotami przetwarzającymi dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych osobowych; w niektórych wypadkach Komisja Europejska wymaga dodatkowo, aby taki podmiot przetwarzający uczestniczył w zatwierdzonych przez nią programach zrzeszających podmioty spoza EOG, których uczestnicy mają obowiązek zapewnienia Danym osobowym taką samą ochronę, jaka przysługuje im w Unii Europejskiej;
   2) stosowanie Standardowych Klauzul Umownych wydanych przez Komisję Europejską wraz z wymaganymi dodatkowymi środkami bezpieczeństwa zapewniają one Danym osobowym taką samą ochronę, jaka przysługuje im w Unii Europejskiej;
   3) stosowanie wiążących reguł korporacyjnych, zatwierdzonych przez właściwy organ nadzorczy.

§9. Bezpieczeństwo danych

1. Administrator na bieżąco prowadzi analizę ryzyka w celu zapewnienia, że dane osobowe przetwarzane są przez niego w sposób bezpieczny – zapewniający przede wszystkim, że dostęp do danych mają jedynie osoby upoważnione i jedynie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania. Administrator dba o to, by wszystkie operacje na danych osobowych były rejestrowane i dokonywane jedynie przez uprawnionych pracowników i współpracowników.
2. Administrator podejmuje wszelkie niezbędne działania, by także jego podwykonawcy i inne podmioty współpracujące dawały gwarancję stosowania odpowiednich środków bezpieczeństwa w każdym przypadku, gdy przetwarzają dane osobowe na zlecenie Administratora.
3. Polityka bezpieczeństwa obejmuje plan zarządzania incydentami bezpieczeństwa, który definiuje procedury identyfikacji incydentów, ich klasyfikacji i oceny ryzyka, podejmowania działań naprawczych, raportowania oraz zapobiegania przyszłym naruszeniom.
4. W przypadku Incydentu Administrator podejmuje niezwłocznie następujące kroki:

    1. analizuje zakres i charakter incydentu, aby ograniczyć jego skutki;
    2. informuje osoby, których dane dotyczą, o incydencie oraz działaniach podjętych w celu ochrony ich danych, a także wskazuje na możliwe konsekwencje i zalecane środki ochrony;
    3. przeprowadza wewnętrzne audyty w celu wyciągnięcia wniosków i zminimalizowania ryzyka wystąpienia podobnych zdarzeń w przyszłości;
    4. zgłasza naruszenie odpowiedniemu organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) w ciągu 72 godzin od wykrycia incydentu, chyba że naruszenie nie stwarza ryzyka naruszenia praw lub wolności osób fizycznych. Zgłoszenie zawiera opis charakteru naruszenia, kategorie i przybliżoną liczbę poszkodowanych osób, możliwe konsekwencje naruszenia, działania podjęte w celu zaradzenia sytuacji.
5. Administrator wdraża i stale doskonali środki ochrony przed cyberzagrożeniami, w tym:
    1. systemy zapobiegania włamaniom (IDS/IPS),
    2. regularne aktualizacje i łatki zabezpieczające,
    3. szyfrowanie danych w tranzycie i w spoczynku,
    4. monitorowanie ruchu sieciowego w celu identyfikacji podejrzanej aktywności,
    5. wdrożenie zasad minimalizacji uprawnień dostępu do danych,
    6. regularne audyty i przeglądy bezpieczeństwa,
    7. szkolenia dla pracowników w zakresie wykrywania phishingu oraz reagowania na incydenty,
    8. testowanie procedur poprzez symulacje incydentów (np. ataki phishingowe, ransomware).
    9. regularne testy penetracyjne w celu oceny podatności systemów,
    10. automatyczne i ręczne testy bezpieczeństwa aplikacji i infrastruktury.
6. Administrator szczególną uwagę zwraca na ochronę przed zagrożeniami komunikacji elektronicznej, takimi jak ataki DDoS, ransomware, phishing, nieautoryzowany dostęp do danych.

§ 10. Tokeny i dane zapisywane w Urządzeniu

1. Aplikacja Usługa GymBox może zapisywać w pamięci urządzenia mobilnego Użytkownika dane techniczne niezbędne do jej prawidłowego działania, w szczególności tzw. **tokeny dostępu,** identyfikatory sesji oraz dane konfiguracyjne.
2. Tokeny służą do utrzymania zalogowania Użytkownika w aplikacji oraz do bezpiecznej komunikacji z serwerem Administratora. Tokeny nie zawierają danych osobowych w postaci umożliwiającej bezpośrednią identyfikację Użytkownika.
3. Tokeny są przechowywane lokalnie w urządzeniu Użytkownika przez okres niezbędny do korzystania z aplikacji lub do momentu wylogowania się z konta. Po tym czasie tokeny są automatycznie usuwane lub zastępowane nowymi.
4. Użytkownik może w dowolnym momencie usunąć dane aplikacji (w tym tokeny) poprzez zmianę ustawień systemowych urządzenia lub odinstalowanie aplikacji.

§10. Zmiany polityki prywatności

Polityka prywatności może być aktualizowana w przypadku zmian technologicznych lub prawnych. Aktualna wersja dokumentu jest publikowana w aplikacji GymBox oraz na stronie internetowej.

Data ostatniej aktualizacji: 17.12.2025 r.

§11. Kontakt w sprawach pomocy

W przypadku pytań lub problemów z aplikacją lub siłownią GymBox, użytkownik może skontaktować się z działem pomocy:

infolinia: +48 800 802 801
e-mail: office@gymbox.pl