

Polityka prywatności LiberUp

Informacja o tym, jakie dane osobowe LiberUp przetwarza, w jakich celach, na jakich podstawach i jakie prawa przysługują osobom, których dane dotyczą.

Wersja: 1.0-draft | Aktualizacja: 2026-08-31

Obowiązuje od: [USTAL DATĘ WEJŚCIA W ŻYCIE]

PROJEKT: przed wejściem dokumentu w życie należy ustalić datę obowiązywania, wskazać faktycznego dostawcę księgowości oraz zweryfikować umowy powierzenia, lokalizacje przetwarzania i ewentualne transfery poza EOG.

1. Administrator danych i kontakt

Administratorem danych osobowych jest LIBERUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, UL. OZORKOWSKA 13A , 95-100 ZGIERZ, NIP: 7322232375, REGON: 54553560900000, KRS: 0001262265, dalej „LiberUp” lub „Administrator”.

W sprawach prywatności można skontaktować się pod adresem contact@liberup.pl albo korespondencyjnie: UL. OZORKOWSKA 13A , 95-100 ZGIERZ. Administrator nie wyznaczył Inspektora Ochrony Danych, ponieważ na dzień wejścia w życie niniejszej Polityki nie zachodzą przesłanki określone w art. 37 ust. 1 RODO.

2. Zakres i źródła danych

Dane otrzymujemy bezpośrednio od Użytkownika podczas rejestracji, zakupów, kontaktu i zarządzania Kontem, automatycznie z urządzenia i połączenia podczas korzystania z serwisu lub aplikacji oraz od operatora płatności w zakresie statusu i identyfikatorów transakcji.

LiberUp nie zakłada przetwarzania szczególnych kategorii danych, takich jak dane o zdrowiu, poglądach lub biometrii. Nie należy przysyłać takich informacji w formularzach ani wiadomościach, jeżeli nie jest to konieczne.

3. Kategorie przetwarzanych danych

- Konto i profil: adres e-mail, skrót hasła, status weryfikacji, język, rola i status Konta oraz opcjonalnie imię, nazwisko, telefon, nazwa firmy i NIP.
- Zamówienia i rozliczenia: identyfikator Użytkownika, pozycje, ilości, ceny, statusy, daty, parametry Licencji i informacje potrzebne do zwrotu.
- Płatności: kwota, status, daty oraz identyfikatory sesji i transakcji Przelewy24 lub Stripe. LiberUp nie przechowuje pełnych danych karty ani danych logowania do banku.
- Licencje i aplikacje: klucz Licencji, Produkt, typ, liczba stanowisk, limit urządzeń, status, terminy oraz historia zdarzeń.
- Urządzenia: techniczny identyfikator i opcjonalna nazwa urządzenia, wersja aplikacji, daty aktywacji i ostatniej komunikacji.
- Bezpieczeństwo: adres IP przy próbach licencyjnych, typ i wynik próby, technicznie skrócone identyfikatory używane przez rate limiting oraz logi serwera i aplikacji.
- Kontakt: imię, adres e-mail, temat i treść wiadomości. Formularz przekazuje wiadomość do skrzynki e-mail i nie zapisuje jej w bazie aplikacji.

- Zgody i preferencje: rodzaj zgody, decyzja, źródło, wersja dokumentu i data; dotyczy to m.in. Regulaminu, newslettera i informacji o Produktach.

4. Cele i podstawy prawne

- Utworzenie Konta, logowanie, obsługa Biblioteki, zamówień, subskrypcji, Licencji, urządzeń, aktualizacji i reklamacji – wykonanie umowy lub działania przed jej zawarciem (art. 6 ust. 1 lit. b RODO).
- Rozliczenia, dokumentacja podatkowa i rachunkowa oraz realizacja obowiązków organów – obowiązek prawny (art. 6 ust. 1 lit. c RODO).
- Bezpieczeństwo, zapobieganie nadużyciom, rate limiting, logi, ustalanie i obrona roszczeń oraz analiza niezawodności – prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO).
- Odpowiedź na wiadomość przed zawarciem umowy – art. 6 ust. 1 lit. b RODO, a w pozostałych sprawach uzasadniony interes polegający na prowadzeniu korespondencji (art. 6 ust. 1 lit. f RODO).
- Newsletter, dobrowolne informacje marketingowe oraz opcjonalna analityka i reklama oparta na cookies – zgoda (art. 6 ust. 1 lit. a RODO oraz właściwe przepisy komunikacji elektronicznej).
- Prowadzenie historii udzielonych i wycofanych zgód – obowiązek wykazania zgodności oraz uzasadniony interes Administratora (art. 6 ust. 1 lit. c i f RODO).

5. Czy podanie danych jest obowiązkowe

Dane oznaczone jako wymagane są potrzebne do utworzenia Konta, zawarcia i wykonania umowy albo obsługi żądania. Ich brak może uniemożliwić rejestrację, zakup, płatność, aktywację lub odpowiedź. Dane profilu oznaczone jako opcjonalne są dobrowolne.

Zgody marketingowe i zgody na opcjonalne cookies są dobrowolne. Ich brak nie ogranicza dostępu do Konta ani zakupionych Produktów.

6. Odbiorcy danych i dostawcy

- OVHcloud — VPS 3 – infrastruktura serwisu i bazy danych; zakres, region przetwarzania i umowę powierzenia należy potwierdzić przed publikacją dokumentu.
- OVHcloud — Zimbra – obsługa wiadomości systemowych, weryfikacji, resetu hasła i formularza kontaktowego.
- PayPro S.A. — Przelewy24; Stripe Payments Europe, Ltd. — Stripe (po aktywacji) – obsługa płatności; PayPro S.A. działa również jako odrębny administrator danych płatnika w zakresie świadczenia usług płatniczych.
- OVHcloud — automatyczna kopia zapasowa VPS, przechowywana i trzykrotnie replikowana na innych serwerach w tym samym centrum danych co VPS w Warszawie, Polska. Retencja: 24 godziny. – kopie zapasowe po wybraniu dostawcy i ustaleniu zakresu.
- Zewnętrzne biuro rachunkowe — w zakresie niezbędnym do prowadzenia księgowości, rozliczeń podatkowych oraz realizacji obowiązków prawnych LiberUp. – rozliczenia i dokumentacja księgowa po wybraniu dostawcy.
- Upoważnieni członkowie zespołu wsparcia i administracji, zgodnie z centralną macierzą uprawnień i zasadą najmniejszych uprawnień.
- Dostawcy obsługi prawnej, bezpieczeństwa lub utrzymania IT, jeżeli ich udział okaże się niezbędny i zostaną objęci odpowiednimi zobowiązaniami.
- Organy publiczne i inne podmioty, gdy ujawnienie danych wynika z obowiązującego prawa.

7. Google Analytics, Google Ads i Google AdSense

Google Analytics, Google Ads i Google AdSense są funkcjami planowanymi, ale obecnie nieaktywnymi. LiberUp nie powinien łączyć ich skryptów ani przekazywać im identyfikatorów przed uzyskaniem wymaganej zgody.

Przed uruchomieniem któregośkolwiek narzędzia należy zaktualizować tę Politykę i Politykę cookies, wskazać dokładną konfigurację, okresy przechowywania, odbiorców, cele, podstawę prawną i mechanizm ewentualnego transferu poza EOG oraz wdrożyć możliwość łatwego wycofania zgody.

8. Przekazywanie danych poza Europejski Obszar Gospodarczy

Serwis, baza danych oraz automatyczne kopie zapasowe są przechowywane w infrastrukturze OVHcloud w Warszawie, Polska. Kopie zapasowe są przechowywane w tym samym centrum danych co VPS. Dane usługi pocztowej OVHcloud Zimbra są hostowane w europejskich centrach danych OVHcloud. OVHcloud może korzystać z podmiotów powiązanych i zatwierdzonych podwykonawców zgodnie z umową powierzenia przetwarzania danych. Jeżeli przetwarzanie będzie wiązało się z przekazaniem danych poza EOG, zastosowanie znajdzie decyzja stwierdzająca odpowiedni stopień ochrony albo standardowe klauzule umowne wraz z wymaganymi zabezpieczeniami.

Planowane usługi Google mogą wiązać się z przetwarzaniem poza EOG. Nie zostaną aktywowane przed udokumentowaniem podstawy i zabezpieczeń transferu.

9. Lokalne przetwarzanie plików JPK

Pliki JPK używane w aplikacjach LiberUp są przetwarzane lokalnie na urządzeniu Użytkownika. Nie są wysyłane do serwerów LiberUp. Serwer może otrzymywać wyłącznie dane potrzebne do Konta, Licencji, wersji, reguł i aktualizacji, bez zawartości plików JPK.

10. Okresy przechowywania

- Konto i profil – dane są przechowywane przez okres korzystania z Konta. Po jego usunięciu dane identyfikacyjne i kontaktowe są niezwłocznie usuwane lub anonimizowane w aktywnej bazie danych. Ich kopie mogą pozostać w automatycznej kopii zapasowej VPS maksymalnie przez 24 godziny, do czasu jej automatycznego zastąpienia. Dane związane z zamówieniami, płatnościami, zgodami, reklamacjami i roszczeniami są przechowywane przez okresy wskazane odrębnie dla tych celów.
- Zamówienia, płatności, zwroty i dokumentacja rozliczeniowa – przez co najmniej 5 lat, licząc od początku roku następującego po roku obrotowym, którego dokumentacja dotyczy. Jeżeli dane są potrzebne w związku z kontrolą, postępowaniem lub roszczeniem, mogą być przechowywane do jego prawomocnego zakończenia albo upływu właściwego terminu przedawnienia.
- Licencje, subskrypcje, urządzenia i zdarzenia – dane potwierdzające zakres uprawnień są przechowywane przez czas wykonywania umowy oraz przez 6 lat, licząc od końca roku kalendarzowego, w którym Licencja lub Subskrypcja wygasła, została anulowana albo odebrana. Dane aktywowanych urządzeń, które nie są już potrzebne do obsługi Licencji lub roszczeń, są usuwane lub anonimizowane w terminie 30 dni od zakończenia Licencji.
- Sesje i tokeny – do chwili wygaśnięcia, wykorzystania, unieważnienia, zmiany hasła albo wylogowania. Nieaktywne rekordy sesji i wykorzystane lub wygasłe tokeny są usuwane w terminie 30 dni.
- Próby licencyjne, adresy IP, logi i rate limiting – informacje o próbach aktywacji, walidacji i dezaktywacji Licencji, w tym adres IP, rodzaj próby i jej wynik, są przechowywane przez 90 dni. Techniczne, skrócone identyfikatory używane przez rate limiting są przechowywane maksymalnie przez 48 godzin. Standardowe logi

aplikacji i serwera są przechowywane przez 30 dni, a logi bezpieczeństwa przez 90 dni. Dane dotyczące konkretnego incydentu mogą być przechowywane dłużej, do zakończenia jego analizy oraz przez okres niezbędny do ustalenia, dochodzenia lub obrony roszczeń.

- Wiadomości kontaktowe i reklamacje – zwykła korespondencja kontaktowa jest przechowywana przez 12 miesięcy od zakończenia sprawy. Korespondencja dotycząca reklamacji, odstąpienia od umowy, zwrotu lub sporu jest przechowywana przez 6 lat, licząc od końca roku kalendarzowego, w którym sprawa została zakończona. Wiadomości są następnie usuwane ze skrzynki OVHcloud Zimbra, chyba że ich dalsze przechowywanie jest wymagane przez prawo albo trwające postępowanie.
- Zgody – aktualne zgody są przechowywane przez czas ich obowiązywania. Informacja o udzieleniu lub wycofaniu zgody marketingowej i newsletterowej jest przechowywana przez 3 lata od jej wycofania lub zastąpienia. Akceptacje Regulaminu, EULA i pozostałych dokumentów związane z Zamówieniem są przechowywane przez okres przechowywania dokumentacji danego Zamówienia lub Licencji.
- Kopie zapasowe – automatyczna kopia całego VPS jest wykonywana codziennie przez OVHcloud i przechowywana przez 24 godziny. Jest trzykrotnie replikowana na innych serwerach w tym samym centrum danych w Warszawie, Polska. Dostęp do kopii jest ograniczony do upoważnionych administratorów za pośrednictwem zabezpieczonego Panelu OVHcloud. LiberUp nie stosuje obecnie dodatkowego szyfrowania aplikacyjnego całej kopii VPS. Kopia jest automatycznie zastępowana kolejną kopią, dlatego dane usunięte z aktywnego systemu mogą pozostawać w backupie maksymalnie przez 24 godziny.

11. Zautomatyzowane decyzje i profilowanie

LiberUp nie podejmuje obecnie wobec Użytkowników decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, które wywołują skutki prawne lub podobnie istotnie wpływają na Użytkownika. Automatyczne mechanizmy bezpieczeństwa mogą krótkotrwale ograniczać liczbę żądań albo odrzucać nieprawidłową aktywację; sporne przypadki można zgłosić do wsparcia.

Profilowanie reklamowe nie jest obecnie aktywne. Przed jego wdrożeniem zakres i skutki zostaną opisane, a wymagane zgody zebrane.

12. Prawa osoby, której dane dotyczą

- prawo dostępu do danych i otrzymania ich kopii;
- prawo sprostowania nieprawidłowych i uzupełnienia niekompletnych danych;
- prawo usunięcia danych, gdy spełnione są przesłanki prawne;
- prawo ograniczenia przetwarzania;
- prawo przenoszenia danych przetwarzanych automatycznie na podstawie zgody lub umowy;
- prawo sprzeciwu wobec przetwarzania opartego na uzasadnionym interesie, a wobec marketingu bezpośredniego – w każdym czasie;
- prawo wycofania zgody w każdym czasie, bez wpływu na zgodność wcześniejszego przetwarzania;
- prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

13. Realizacja praw i weryfikacja tożsamości

Wnioski można kierować na contact@liberup.pl. LiberUp może poprosić o informacje niezbędne do bezpiecznego potwierdzenia tożsamości, ale nie będzie zbierać w tym celu nadmiarowych danych. Odpowiedź zostanie udzielona w terminie wynikającym z RODO.

Nie każde żądanie usunięcia oznacza natychmiastowe usunięcie wszystkich rekordów. Dane mogą pozostać, jeżeli dalsze przechowywanie jest niezbędne z uwagi na obowiązek prawny, rozliczenia, bezpieczeństwo lub ustalenie, dochodzenie albo obronę roszczeń.

14. Bezpieczeństwo danych

LiberUp stosuje środki adekwatne do ryzyka, w tym kontrolę dostępu według ról, haszowanie haseł, ochronę sekretów po stronie serwera, szyfrowane połączenia, ograniczanie liczby żądań, rejestrowanie zdarzeń licencyjnych oraz procedury aktualizacji i kopii zapasowych. Zakres środków jest okresowo przeglądany.

Żadna metoda transmisji lub przechowywania nie gwarantuje całkowitego bezpieczeństwa. Podejrzanie naruszenia można zgłosić na adres do spraw prywatności.

15. Dane dzieci

Oferta LiberUp nie jest kierowana do dzieci. Jeżeli Administrator stwierdzi, że dane dziecka zostały przekazane bez wymaganej podstawy lub zgody przedstawiciela ustawowego, podejmie działania w celu ich usunięcia albo wyjaśnienia sytuacji.

16. Zmiany i wersjonowanie Polityki

Polityka otrzymuje numer wersji i datę wejścia w życie. Istotne zmiany dotyczące trwałego przetwarzania będą komunikowane w odpowiedni sposób przed ich zastosowaniem. Archiwalne wersje będą dostępne w Centrum prawnym.

Powiązane dokumenty tej wersji

[Regulamin LiberUp — PDF](#) · [Polityka cookies — PDF](#) · [Umowa licencyjna EULA — PDF](#) · [Reklamacje i odstąpienie — PDF](#) · [Informacja o dostępności — PDF](#)

liberup.pl/legal/archive