POLITYKA PRYWATNOŚCI APLIKACJI YOUR MONEY HANDLED

§ 1. Postanowienia ogólne

1. Niniejsza Polityka Prywatności (dalej: „Polityka Prywatności") określa zasady przetwarzania i ochrony danych osobowych Usługobiorców korzystających z aplikacji „Your Money Handled" (dalej: „Aplikacja") dostępnej pod adresem app.yourmoneyhandled.pl oraz strony internetowej yourmoneyhandled.pl (dalej łącznie: „Serwis").
2. Polityka Prywatności stanowi wypełnienie obowiązku informacyjnego, o którym mowa w art. 13 i art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej: „RODO").
3. Polityka Prywatności jest dokumentem, o którym mowa w Regulaminie Aplikacji Your Money Handled (dalej: „Regulamin"). Terminy pisane wielką literą, niezdefiniowane w niniejszej Polityce Prywatności, mają znaczenie nadane im w Regulaminie.
4. Administrator dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, że zbierane przez niego dane są przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, oraz przechowywane w formie umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 2. Administrator danych osobowych

1. Administratorem danych osobowych przetwarzanych w związku z korzystaniem z Serwisu jest **[DO UZUPEŁNIENIA PRZEZ JORGO - IMIĘ I NAZWISKO]**, prowadzący działalność nierejestrowaną w rozumieniu art. 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (dalej: „Administrator").
2. Dane kontaktowe Administratora:
    1. adres do korespondencji: **[DO UZUPEŁNIENIA PRZEZ JORGO - ADRES DO KORESPONDENCJI]**,
    2. adres poczty elektronicznej: contact@yourmoneyhandled.pl,
    3. numer telefonu: **[DO UZUPEŁNIENIA PRZEZ JORGO - NUMER TELEFONU]**.

3. Administrator nie wyznaczył Inspektora Ochrony Danych (IOD). We wszelkich sprawach związanych z przetwarzaniem danych osobowych Usługobiorca może kontaktować się bezpośrednio z Administratorem za pośrednictwem danych kontaktowych wskazanych w ust. 2 powyżej.

§ 3. Definicje

Użyte w Polityce Prywatności wyrazy pisane wielką literą, o ile nie zostały zdefiniowane w Regulaminie, mają następujące znaczenie:

1. **Administrator** – termin zdefiniowany w § 2 ust. 1 Polityki Prywatności;
2. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej w rozumieniu art. 4 pkt 1 RODO;
3. **Pliki cookies (ciasteczka)** – małe pliki tekstowe przechowywane na urządzeniu końcowym Usługobiorcy podczas korzystania z Serwisu;
4. **Podmiot przetwarzający (procesor)** – podmiot, który przetwarza dane osobowe w imieniu Administratora na podstawie umowy powierzenia przetwarzania danych osobowych;
5. **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych w rozumieniu art. 4 pkt 2 RODO;
6. **RODO** – termin zdefiniowany w § 1 ust. 2 Polityki Prywatności;
7. **UODO** – Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

§ 4. Zakres zbieranych danych osobowych

1. Administrator zbiera i przetwarza następujące kategorie danych osobowych Usługobiorców:

A. Dane rejestracyjne

2. W celu założenia Konta i korzystania z Aplikacji Usługobiorca podaje:
    1. adres poczty elektronicznej (e-mail),
    2. hasło (przechowywane wyłącznie w formie zahashowanej - Administrator nie ma dostępu do hasła w postaci jawnej),
    3. imię lub pseudonim (podawane podczas procesu wstępnej konfiguracji Konta).
3. W przypadku rejestracji za pośrednictwem konta Google, Administrator otrzymuje z profilu Google następujące dane:
    1. adres poczty elektronicznej,
    2. imię (z profilu Google).

B. Dane finansowe wprowadzane przez Usługobiorcę

4. W ramach korzystania z funkcjonalności Aplikacji Usługobiorca może dobrowolnie wprowadzać następujące dane:
    1. transakcje (wydatki i przychody),
    2. budżety,
    3. cele oszczędnościowe,
    4. płatności cykliczne,
    5. plany spłat zobowiązań,
    6. listy zakupów,
    7. konta finansowe (nazwy i salda - Aplikacja **nie** zbiera numerów kont bankowych),
    8. karty lojalnościowe (zdjęcia i/lub numery),
    9. kategorie i grupy wydatków.
5. Dane finansowe, o których mowa w ust. 4 powyżej, są wprowadzane ręcznie przez Usługobiorcę. Aplikacja nie pobiera danych automatycznie z rachunków bankowych ani innych instytucji finansowych.

C. Dane techniczne i analityczne

6. Podczas korzystania z Serwisu automatycznie zbierane są następujące dane techniczne:
    1. adres IP,
    2. typ i wersja przeglądarki internetowej,
    3. typ urządzenia i system operacyjny,
    4. dane o sposobie korzystania z Aplikacji (np. odwiedzane ekrany, kliknięcia, czas spędzony w Aplikacji) - zbierane za pomocą narzędzia PostHog.
7. Dane techniczne i analityczne są zbierane w celu zapewnienia prawidłowego funkcjonowania Serwisu, analizy ruchu oraz ulepszania Aplikacji.

D. Dane płatnicze

8. Dane płatnicze (dane karty płatniczej, dane rachunku bankowego) są przetwarzane **wyłącznie** przez operatora płatności Stripe i **nie** są przechowywane przez Administratora.
9. Administrator otrzymuje od Stripe wyłącznie następujące informacje:
    1. status płatności (powodzenie/niepowodzenie),
    2. datę płatności,
    3. kwotę płatności,
    4. identyfikator klienta w systemie Stripe.

§ 5. Cele i podstawy prawne przetwarzania danych osobowych

1. Administrator przetwarza dane osobowe Usługobiorców w następujących celach i na następujących podstawach prawnych:

A. Wykonanie umowy - art. 6 ust. 1 lit. b RODO

2. Przetwarzanie danych jest niezbędne do wykonania Umowy, której stroną jest Usługobiorca, lub do podjęcia działań na żądanie Usługobiorcy przed zawarciem Umowy. Obejmuje to w szczególności:
    1. rejestrację i utrzymanie Konta w Aplikacji,
    2. świadczenie Usługi korzystania z Aplikacji (w tym przechowywanie i wyświetlanie danych finansowych wprowadzonych przez Usługobiorcę),
    3. obsługę płatności za Usługę w wariancie Pro,
    4. komunikację z Usługobiorcą w sprawach związanych z funkcjonowaniem Aplikacji i realizacją Umowy,
    5. realizację prawa do eksportu danych (art. 4 § 17 Regulaminu).
3. **Okres przechowywania:** przez czas trwania Umowy oraz przez okres 90 (dziewięćdziesięciu) dni archiwizacji po usunięciu Konta (zgodnie z § 11 ust. 8 Regulaminu).

B. Prawnie uzasadniony interes Administratora - art. 6 ust. 1 lit. f RODO

4. Administrator przetwarza dane osobowe w celach wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, w szczególności:
    1. analityka produktowa i ulepszanie Aplikacji (za pomocą narzędzia PostHog),
    2. zapewnienie bezpieczeństwa Serwisu i ochrona przed nadużyciami,
    3. ustalenie, dochodzenie lub obrona przed roszczeniami.
5. **Okres przechowywania:** do czasu wniesienia skutecznego sprzeciwu przez Usługobiorcę (art. 21 RODO) lub do czasu upływu terminów przedawnienia roszczeń wynikających z przepisów prawa (co do zasady: 6 lat dla roszczeń majątkowych, 3 lata dla roszczeń związanych z prowadzeniem działalności gospodarczej).

C. Zgoda - art. 6 ust. 1 lit. a RODO

6. W przypadku wyrażenia dobrowolnej zgody przez Usługobiorcę, Administrator przetwarza dane osobowe w następujących celach:
    1. stosowanie analitycznych plików cookies (jeżeli wdrożony jest mechanizm zarządzania zgodami - consent banner),
    2. wysyłka newslettera oraz obsługa listy oczekujących (waitlista) za pośrednictwem usługi MailerLite.

7. **Okres przechowywania:** do czasu wycofania zgody przez Usługobiorcę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

D. Obowiązek prawny - art. 6 ust. 1 lit. c RODO

8. Administrator przetwarza dane osobowe w zakresie, w jakim jest to niezbędne do wypełnienia obowiązków prawnych ciążących na Administratorze, w szczególności:
    1. przechowywanie dokumentacji podatkowej i rachunkowej (jeżeli ma zastosowanie),
    2. realizacja obowiązków wynikających z RODO (np. obsługa żądań realizacji praw podmiotów danych).
9. **Okres przechowywania:** przez okres wymagany przepisami prawa (w szczególności: 5 lat od końca roku kalendarzowego, w którym upłynął termin płatności podatku - w zakresie dokumentacji podatkowej).

§ 6. Odbiorcy danych osobowych (podmioty przetwarzające i niezależni administratorzy)

1. Administrator może udostępniać dane osobowe Usługobiorców następującym kategoriom odbiorców:

A. Supabase Inc.

2. **Rola:** podmiot przetwarzający (procesor).
3. **Siedziba:** San Francisco, CA, Stany Zjednoczone Ameryki.
4. **Zakres danych:** wszystkie dane Usługobiorcy (dane rejestracyjne, dane finansowe wprowadzone przez Usługobiorcę, dane uwierzytelniające).
5. **Cel:** zapewnienie infrastruktury backendowej, bazy danych oraz usługi uwierzytelniania (Supabase Auth).
6. **Lokalizacja serwerów: [DO UZUPEŁNIENIA PRZEZ JORGO - REGION SERWERA SUPABASE, np. AWS eu-central-1 (Frankfurt, Niemcy)]**.
7. **Podstawa transferu danych do USA:** Standardowe Klauzule Umowne (SCC) przyjęte decyzją wykonawczą Komisji Europejskiej (UE) 2021/914, oraz/lub uczestnictwo w EU-US Data Privacy Framework (DPF), zgodnie z decyzją wykonawczą Komisji Europejskiej z dnia 10 lipca 2023 r. w sprawie odpowiedniego stopnia ochrony danych osobowych zapewnionego przez Ramy ochrony danych UE–USA.

B. PostHog Inc.

8. **Rola:** podmiot przetwarzający (procesor).

9. **Siedziba:** San Francisco, CA, Stany Zjednoczone Ameryki.
10. **Zakres danych:** dane techniczne i analityczne (adres IP, typ przeglądarki, dane o sposobie korzystania z Aplikacji); dane są anonimizowane tam, gdzie jest to możliwe.
11. **Cel:** analityka produktowa i ulepszanie Aplikacji.
12. **Lokalizacja serwerów: [DO UZUPEŁNIENIA PRZEZ JORGO - czy PostHog jest hostowany na serwerach EU (PostHog Cloud EU) czy US]**.
13. **Podstawa transferu danych do USA** (jeżeli serwery znajdują się w USA): Standardowe Klauzule Umowne (SCC) oraz/lub EU-US Data Privacy Framework (DPF).

C. Stripe Inc. / Stripe Payments Europe, Ltd.

14. **Rola:** niezależny administrator danych (w zakresie danych płatniczych).
15. **Siedziba europejska:** Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irlandia.
16. **Zakres danych:** dane płatnicze (dane karty płatniczej), adres e-mail Usługobiorcy.
17. **Cel:** obsługa płatności za Usługę w wariancie Pro.
18. **Uwaga:** Stripe przetwarza dane płatnicze jako niezależny administrator danych na podstawie własnej polityki prywatności dostępnej pod adresem: https://stripe.com/privacy. Administrator przekazuje Stripe wyłącznie dane niezbędne do realizacji płatności.

D. Vercel Inc.

19. **Rola:** podmiot przetwarzający (procesor).
20. **Siedziba:** San Francisco, CA, Stany Zjednoczone Ameryki.
21. **Zakres danych:** adres IP, dane techniczne (logi serwera).
22. **Cel:** hosting strony internetowej yourmoneyhandled.pl oraz Aplikacji webowej.
23. **Podstawa transferu danych do USA:** Standardowe Klauzule Umowne (SCC) oraz/lub EU-US Data Privacy Framework (DPF).

E. Google LLC

24. **Rola:** niezależny administrator danych (w zakresie danych związanych z usługą Google OAuth).
25. **Siedziba:** Mountain View, CA, Stany Zjednoczone Ameryki.
26. **Zakres danych:** adres e-mail, imię (z profilu Google) - dotyczy wyłącznie Usługobiorców korzystających z rejestracji za pośrednictwem konta Google.
27. **Cel:** umożliwienie rejestracji i logowania za pośrednictwem konta Google (Google OAuth).
28. **Uwaga:** Google przetwarza dane jako niezależny administrator danych na podstawie własnej polityki prywatności dostępnej pod adresem: https://policies.google.com/privacy.

F. UAB MailerLite

29. **Rola:** podmiot przetwarzający (procesor).
30. **Siedziba:** J. Basanavičiaus g. 15, LT-03108 Vilnius, Litwa (Unia Europejska).
31. **Zakres danych:** adres e-mail.
32. **Cel:** obsługa newslettera i listy oczekujących (waitlista).
33. **Podstawa transferu:** dane przetwarzane w ramach Europejskiego Obszaru Gospodarczego (EOG) - brak transferu danych poza EOG.

G. Inne podmioty

34. Administrator może udostępnić dane osobowe Usługobiorców również:
    1. podmiotom uprawnionym do ich otrzymania na podstawie obowiązujących przepisów prawa (np. sądy, organy ścigania, organy administracji publicznej),
    2. podmiotom świadczącym na rzecz Administratora usługi doradcze, prawne, księgowe - w zakresie niezbędnym do realizacji tych usług.

§ 7. Transfer danych osobowych do państw trzecich

1. W związku z korzystaniem z usług podmiotów przetwarzających, o których mowa w § 6, dane osobowe Usługobiorców mogą być przekazywane do Stanów Zjednoczonych Ameryki (USA), które są państwem trzecim w rozumieniu RODO.
2. Przekazanie danych osobowych do USA odbywa się na podstawie:
    1. decyzji wykonawczej Komisji Europejskiej z dnia 10 lipca 2023 r. stwierdzającej odpowiedni stopień ochrony danych osobowych zapewniany przez Ramy ochrony danych UE–USA (EU-US Data Privacy Framework) - w odniesieniu do podmiotów certyfikowanych w ramach DPF (art. 45 RODO),
    2. Standardowych Klauzul Umownych (SCC) przyjętych decyzją wykonawczą Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. - w odniesieniu do podmiotów nieobjętych DPF lub jako dodatkowe zabezpieczenie (art. 46 ust. 2 lit. c RODO).
3. Usługobiorca ma prawo uzyskać kopię danych osobowych przekazywanych do państwa trzeciego oraz informację o zastosowanych zabezpieczeniach, kontaktując się z Administratorem za pośrednictwem danych kontaktowych wskazanych w § 2 ust. 2 Polityki Prywatności.

§ 8. Prawa Usługobiorcy

1. Usługobiorcy przysługują następujące prawa w związku z przetwarzaniem jego danych osobowych:

1. **Prawo dostępu do danych** (art. 15 RODO) - Usługobiorca ma prawo uzyskać od Administratora potwierdzenie, czy przetwarzane są dane osobowe jego dotyczące, a jeżeli ma to miejsce, ma prawo uzyskać dostęp do nich oraz informacje wskazane w art. 15 RODO.
2. **Prawo do sprostowania danych** (art. 16 RODO) - Usługobiorca ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących go danych osobowych, które są nieprawidłowe, oraz uzupełnienia niekompletnych danych osobowych.
3. **Prawo do usunięcia danych („prawo do bycia zapomnianym")** (art. 17 RODO) - Usługobiorca ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących go danych osobowych, w przypadkach wskazanych w art. 17 ust. 1 RODO, z zastrzeżeniem wyjątków określonych w art. 17 ust. 3 RODO.
4. **Prawo do ograniczenia przetwarzania** (art. 18 RODO) - Usługobiorca ma prawo żądania od Administratora ograniczenia przetwarzania w przypadkach wskazanych w art. 18 ust. 1 RODO.
5. **Prawo do przenoszenia danych** (art. 20 RODO) - Usługobiorca ma prawo otrzymać dotyczące go dane osobowe w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (JSON lub CSV) oraz ma prawo przesłać te dane innemu administratorowi bez przeszkód ze strony Administratora. Aplikacja umożliwia eksport danych na warunkach określonych w § 4 ust. 17 oraz § 11 ust. 9 Regulaminu.
6. **Prawo do sprzeciwu** (art. 21 RODO) - Usługobiorca ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jego szczególną sytuacją - wobec przetwarzania dotyczących go danych osobowych opartego na art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes Administratora). Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności Usługobiorcy, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
7. **Prawo do wycofania zgody** (art. 7 ust. 3 RODO) - w zakresie, w jakim przetwarzanie danych osobowych odbywa się na podstawie zgody, Usługobiorca ma prawo do wycofania zgody w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
8. **Prawo do złożenia skargi do organu nadzorczego** (art. 77 RODO) - Usługobiorca ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (UODO), ul. Stawki 2, 00-193 Warszawa, strona internetowa: https://uodo.gov.pl, jeżeli uzna, że przetwarzanie dotyczących go danych osobowych narusza przepisy RODO.

2. W celu skorzystania z praw, o których mowa w ust. 1 powyżej, Usługobiorca powinien skontaktować się z Administratorem za pośrednictwem danych kontaktowych wskazanych w § 2 ust. 2 Polityki Prywatności.

3. Administrator udziela odpowiedzi na żądanie Usługobiorcy bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, o czym Administrator informuje Usługobiorcę w terminie miesiąca od otrzymania żądania.
4. Realizacja praw Usługobiorcy jest wolna od opłat. Jeżeli jednak żądania Usługobiorcy są ewidentnie nieuzasadnione lub nadmierne (w szczególności ze względu na swój ustawiczny charakter), Administrator może pobrać rozsądną opłatę uwzględniającą administracyjne koszty udzielenia informacji lub odmówić podjęcia działań w związku z żądaniem - zgodnie z art. 12 ust. 5 RODO.

§ 9. Pliki cookies

1. Serwis wykorzystuje pliki cookies (ciasteczka), które są przechowywane na urządzeniu końcowym Usługobiorcy.
2. Pliki cookies stosowane w Serwisie dzielą się na następujące kategorie:

A. Pliki cookies niezbędne (strictly necessary)

3. Pliki cookies niezbędne do prawidłowego funkcjonowania Serwisu, w szczególności:
    1. pliki cookies sesyjne (utrzymanie sesji zalogowanego Usługobiorcy),
    2. pliki cookies uwierzytelniające (Supabase Auth).
4. Pliki cookies niezbędne nie wymagają zgody Usługobiorcy, ponieważ są konieczne do świadczenia Usługi, o którą Usługobiorca wyraźnie poprosił (art. 173 ust. 3 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne).

B. Pliki cookies funkcjonalne

5. Pliki cookies służące do zapamiętania preferencji Usługobiorcy (np. preferencje wyświetlania, tryb ciemny/jasny).
6. Pliki cookies funkcjonalne nie wymagają zgody Usługobiorcy, ponieważ służą wyłącznie do zapamiętania ustawień wybranych przez Usługobiorcę.

C. Pliki cookies analityczne

7. Pliki cookies służące do zbierania danych o sposobie korzystania z Serwisu, w szczególności pliki cookies narzędzia PostHog.
8. Pliki cookies analityczne wymagają uprzedniej zgody Usługobiorcy (wyrażonej za pośrednictwem mechanizmu zarządzania zgodami - consent banner) lub są stosowane na

podstawie prawnie uzasadnionego interesu Administratora z możliwością wniesienia sprzeciwu (opt-out).

D. Zarządzanie plikami cookies

9. Usługobiorca może w dowolnym momencie zmienić ustawienia dotyczące plików cookies w swojej przeglądarce internetowej, w tym zablokować lub usunąć pliki cookies. Szczegółowe informacje o zarządzaniu plikami cookies dostępne są w dokumentacji przeglądarki internetowej Usługobiorcy.
10. Ograniczenie stosowania plików cookies może wpłynąć na niektóre funkcjonalności Serwisu.

§ 10. Bezpieczeństwo danych osobowych

1. Administrator stosuje odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator stosuje w szczególności następujące środki bezpieczeństwa:
    1. **Szyfrowanie transmisji danych** - komunikacja między urządzeniem Usługobiorcy a serwerami Serwisu jest szyfrowana z wykorzystaniem protokołu SSL/TLS.
    2. **Hashowanie haseł** - hasła Usługobiorców są przechowywane wyłącznie w formie zahashowanej (algorytm bcrypt realizowany przez Supabase Auth). Administrator nie ma dostępu do haseł w postaci jawnej.
    3. **Row Level Security (RLS)** - na poziomie bazy danych (Supabase) wdrożono mechanizm Row Level Security, zapewniający, że każdy Usługobiorca ma dostęp wyłącznie do własnych danych.
    4. **Regularne kopie zapasowe (backupy)** - dane są regularnie archiwizowane w celu zapewnienia ich odtwarzalności w przypadku awarii.
    5. **Zasada minimalizacji danych** - Administrator zbiera wyłącznie dane niezbędne do realizacji celów przetwarzania określonych w § 5 Polityki Prywatności.

§ 11. Profilowanie i zautomatyzowane podejmowanie decyzji

1. Administrator **nie** podejmuje decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywoływałyby wobec Usługobiorcy skutki prawne lub w podobny sposób istotnie na niego wpływały (art. 22 RODO).
2. Dane analityczne zbierane za pomocą narzędzia PostHog mogą być wykorzystywane do analizy statystycznej i segmentacji użytkowników w celu ulepszania Aplikacji, jednakże

analiza ta nie prowadzi do podejmowania zautomatyzowanych decyzji wywołujących skutki prawne wobec Usługobiorcy.

§ 12. Okres przechowywania danych osobowych

1. Dane osobowe Usługobiorców są przechowywane przez okres niezbędny do realizacji celów, dla których zostały zebrane, zgodnie z następującymi zasadami:

Cel przetwarzania	Okres przechowywania
Wykonanie Umowy (świadczenie Usługi)	Przez czas trwania Umowy + 90 dni archiwizacji po usunięciu Konta
Prawnie uzasadniony interes (analityka, bezpieczeństwo)	Do czasu wniesienia skutecznego sprzeciwu lub upływu terminów przedawnienia roszczeń
Zgoda (newsletter, cookies analityczne)	Do czasu wycofania zgody
Obowiązek prawny (dokumentacja podatkowa)	Zgodnie z wymogami prawa (co do zasady 5 lat od końca roku podatkowego)

2. Po upływie okresu przechowywania dane osobowe są niezwłocznie usuwane lub anonimizowane w sposób uniemożliwiający identyfikację Usługobiorcy.

§ 13. Zmiany Polityki Prywatności

1. Administrator zastrzega sobie prawo do wprowadzania zmian w Polityce Prywatności, w szczególności w przypadku:
    1. zmian w obowiązujących przepisach prawa dotyczących ochrony danych osobowych,
    2. zmian w zakresie przetwarzanych danych osobowych, celów lub podstaw prawnych przetwarzania,
    3. zmian technologicznych wpływających na sposób przetwarzania danych osobowych,
    4. zmian w zakresie podmiotów przetwarzających lub odbiorców danych.
2. O zmianach Polityki Prywatności Usługobiorca zostanie poinformowany:
    1. za pośrednictwem komunikatu wyświetlanego w Aplikacji, oraz/lub
    2. za pośrednictwem wiadomości przesłanej na adres poczty elektronicznej Usługobiorcy.
3. Zmieniona Polityka Prywatności wchodzi w życie w terminie wskazanym w komunikacie o zmianach, nie wcześniej jednak niż po upływie 14 (czternastu) dni od dnia poinformowania Usługobiorcy o zmianach.

§ 14. Postanowienia końcowe

1. Polityka Prywatności obowiązuje od dnia **[DO UZUPEŁNIENIA PRZEZ JORGO - DATA WEJŚCIA W ŻYCIE]** r.
2. W sprawach nieuregulowanych w Polityce Prywatności zastosowanie mają przepisy RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz inne powszechnie obowiązujące przepisy prawa polskiego i unijnego dotyczące ochrony danych osobowych.
3. Polityka Prywatności jest dostępna pod adresem: **https://yourmoneyhandled.pl/legal/polityka-prywatnosci.html** oraz w Aplikacji.

Uwagi dla Jorgo

Poniżej znajduje się lista wszystkich miejsc w Polityce Prywatności wymagających uzupełnienia:

Dane osobowe Administratora

1. **§ 2 ust. 1** - `[DO UZUPEŁNIENIA PRZEZ JORGO – IMIĘ I NAZWISKO]` - Twoje pełne imię i nazwisko (spójne z Regulaminem § 1 ust. 4).
2. **§ 2 ust. 2 pkt 1** - `[DO UZUPEŁNIENIA PRZEZ JORGO – ADRES DO KORESPONDENCJI]` - adres do korespondencji (spójne z Regulaminem § 1 ust. 4).
3. **§ 2 ust. 2 pkt 3** - `[DO UZUPEŁNIENIA PRZEZ JORGO – NUMER TELEFONU]` - numer telefonu kontaktowego (spójne z Regulaminem § 1 ust. 5 pkt 3).

Dane techniczne do zweryfikowania

4. **§ 6 ust. 6** (Supabase) - `[DO UZUPEŁNIENIA PRZEZ JORGO – REGION SERWERA SUPABASE]` - sprawdź w panelu Supabase, w jakim regionie AWS hostowany jest Twój projekt. Jeśli to `eu-central-1` (Frankfurt), wpisz: *„AWS eu-central-1 (Frankfurt, Niemcy)"*. Ma to znaczenie dla transferu danych poza EOG.
5. **§ 6 ust. 12** (PostHog) - `[DO UZUPEŁNIENIA PRZEZ JORGO – czy PostHog na serwerach EU czy US]` - jeśli korzystasz z PostHog Cloud EU (serwery w UE), transfer danych poza EOG nie występuje i podstawa transferu do USA jest zbędna. Sprawdź w ustawieniach PostHog region hostingu.

Daty i linki

6. **§ 14 ust. 1** - `[DO UZUPEŁNIENIA PRZEZ JORGO – DATA WEJŚCIA W ŻYCIE]` - data wejścia w życie Polityki Prywatności (powinna być taka sama lub wcześniejsza niż data wejścia w życie Regulaminu).

7. **§ 14 ust. 3** - `[DO UZUPEŁNIENIA PRZEZ JORGO – URL]` - adres URL, pod którym będzie opublikowana Polityka Prywatności (np. `yourmoneyhandled.pl/privacy`).

Dodatkowe rekomendacje

- **Consent banner (baner zgód):** Jeżeli stosujesz pliki cookies analityczne PostHog, zaimplementuj mechanizm zarządzania zgodami (consent banner/cookie banner) przed wdrożeniem produkcyjnym. Bez tego pliki cookies analityczne mogą być stosowane wyłącznie na podstawie uzasadnionego interesu z opcją opt-out, co jest mniej bezpieczne prawnie.
- **Rejestr czynności przetwarzania (RCP):** Na podstawie art. 30 RODO Administrator powinien prowadzić rejestr czynności przetwarzania. Choć istnieje wyjątek dla podmiotów zatrudniających mniej niż 250 osób, wyjątek ten **nie** ma zastosowania, gdy przetwarzanie dotyczy danych, które nie są sporadyczne (a w przypadku aplikacji SaaS jest to przetwarzanie ciągłe). Zalecam przygotowanie prostego RCP.
- **Umowy powierzenia przetwarzania danych (DPA):** Upewnij się, że masz podpisane Data Processing Agreements z Supabase, PostHog, Vercel i MailerLite. Większość z nich udostępnia DPA online (do zaakceptowania w panelu klienta).
- **Spójność z Regulaminem:** Polityka Prywatności odwołuje się do Regulaminu (§ 1 ust. 3). Pamiętaj, aby w Regulaminie (§ 14) wpisać prawidłowy link do Polityki Prywatności po jej opublikowaniu.
- **Przyszłe zmiany (Plaid):** Jeżeli w przyszłości wdrożysz integrację z Plaid (automatyczne pobieranie transakcji z banków), Polityka Prywatności będzie wymagała istotnej aktualizacji - dodanie Plaid jako podmiotu przetwarzającego, rozszerzenie zakresu danych o dane z rachunków bankowych, dodanie odpowiednich podstaw prawnych. **Zdecydowanie zalecam konsultację z prawnikiem specjalizującym się w fintech/ochronie danych przed wdrożeniem Plaid.**