



21 kwietnia 2020 r.

Weryfikacja Tożsamości przez GdziePoLek

Dokument dla potrzeb wykorzystania procesu dla zewnętrznych partnerów w ramach projektu badawczego opracowanego przez GdziePoLek.

1. Opis usługi niekomercyjnej
2. Proces weryfikacji i szczegóły techniczne
3. Opcjonalne dodatkowe usługi komercyjne
4. Regulamin (wersja robocza)

Gdziekolwiek w dokumencie mowa o **GdziePoLek**, chodzi o podmiot:

GdziePoLek spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie przy pl. Piłsudskiego 3, kod pocztowy 00-078, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000530013, NIP 525-259-99-96, REGON 360126624. GdziePoLek.

Podstawową działalnością GdziePoLek jest pomoc pacjentom w znalezieniu leków w stacjonarnych aptekach. Na moment powstanie dokumentu GdziePoLek jest zintegrowany z prawie 1300 aptekami i obsługuje około 1,5 mln użytkowników miesięcznie.



1. Opis usługi niekomercyjnej

GdziePoLek stworzył w ramach projektu badawczego proces weryfikacji tożsamości użytkownika przy użyciu **Profilu Zaufanego**, a dokładnie podpisania za jego pośrednictwem dokumentów.

W uproszczeniu proces wygląda następująco:

1. GdziePoLek dostarcza użytkownikowi dokument tekstowy do podpisania
2. Użytkownik podpisuje przekazany dokument na stronie Profilu Zaufanego
3. Użytkownik przekazuje podpisany dokument
4. GdziePoLek weryfikuje, że podpis jest prawidłowy i uznaje dane z podpisu za potwierdzone

Dla samego GdziePoLek istotna jest jedynie weryfikacja, że użytkownik jest właścicielem numeru PESEL, co jest potrzebne dla bezpieczeństwa procesu zapytań o e-recepty.

Ten dokument opisuje wersję procesu udostępnioną **partnerom zewnętrznym**. Pozwala ona na:

- Weryfikację wybranego zakresu danych, który może obejmować: fakt samego posiadania profilu zaufanego, imię, nazwisko, data urodzenia, płeć, PESEL w formie bezpowrotnie zaszyfrowanej (hash)
- Wykorzystanie GdziePoLek pozwala stronie trzeciej pozyskać od użytkownika tylko rzeczywiście potrzebne dane, na przykład wiek; GdziePoLek nie przekaze stronie trzeciej pozostałych danych, więc użytkownik może pozostać anonimowy dla danego partnera

W przypadku procesu dla partnerów zewnętrznych GdziePoLek nie przechowuje danych weryfikowanych użytkowników.

Korzystanie z procesu jest bezpłatne niezależnie od podmiotu lub wolumenu operacji.

Opcjonalne dodatkowe wsparcie ze strony zespołu GdziePoLek, dopasowanie produktu do potrzeb partnera lub zawarcie indywidualnej umowy jest płatne.



2. Proces weryfikacji i szczegóły techniczne

Poniżej przedstawione są wszystkie kroki niezbędne do uruchomienia usługi dla domeny posiadanej przez partnera zewnętrznego i dokonania weryfikacji dla użytkownika.

Rejestracja strony korzystającej z API

Należy zarejestrować konto użytkownika na GdziePoLek.pl. Możliwe jest użycie loginu zewnętrznego (Facebook lub Google).

Po rejestracji użytkownik może przeglądać listę zarejestrowanych dla potrzeb korzystania z API stron pod adresem:

<https://www.gdziepolek.pl/partnerchains/list>

Przed dodaniem pierwszej nowej strony konieczna jest **weryfikacja tożsamości**. GdziePoLek zapisze dane osoby rejestrującej stronę wykorzystującą API.

Dodania nowej strony wymaga podania takich danych jak:

Nazwa: dowolne określenie tworzonej pozycji. Tworzony jest z niej automatycznie **unikalny Id**, który będzie widoczny w adresie strony na GdziePoLek weryfikującej tożsamość dla partnera. Można stworzyć kilka pozycji dla jednej domeny, ale należy pamiętać, że przesyłany hash PESEL będzie inny dla każdej z nich.

Domena: po weryfikacji tożsamości użytkownik będzie przekierowany na z góry określony adres w ramach tej domeny

Podmiot i jego adres: użytkownik zostanie poinformowany, że za podaną domenę odpowiada wskazany podmiot i że to on będzie administratorem przekazanych danych

Telefon kontaktowy: nie jest widoczny dla użytkowników

Po rejestracji, stronie zostanie również automatycznie przypisany **Klucz do API**, którym będzie autoryzować sprawdzenie wyników weryfikacji.



Po dodaniu strony wszystkie potrzebne informacje można znaleźć w widoku „szczegóły”:

Szczegóły domeny korzystającej z API	
Nazwa	Goldenberry
Domena	www.goldenberry.eu
Id	goldenberry
Podmiot	Goldenberry sp. z o.o. sp. kom. pl. Piłsudskiego 3, 00-095 Warszawa
API aktywne	TAK
Url wywoływany po zakończeniu identyfikacji	https://www.goldenberry.eu/IdValidationCompleted wywołanie POST
Klucz do API	grtgriji5t34tdgdfgdfg używaj go tylko po stronie serwera
Telefon kontaktowy	+48 22 449 00 50

Przekierowanie użytkownika do GdziePoLek w celu weryfikacji danych

Partner umieszcza w wybranym przez siebie procesie odnośnik do GdziePoLek o następującym formacie URL (wartości dla parametrów są przykładowe):

<https://www.gdziepolek.pl/weryfikacja-tozsamosci?scope=flhbs&partner=id-partnera&id=abcdabcdabcd>

Parametry to:

partner (string): unikalny Id partnera widoczny po rejestracji strony korzystającej z API w widoku szczegółów (wiersz „Id”)



id (string): Id operacji sprawdzenia tożsamości stworzony po stronie partnera dla danego użytkownika; może to być jednorazowy guid lub hash Id użytkownika, nie powinno być możliwe zgadnięcie id operacji dla innego użytkownika lub id kolejnej operacji. Nie należy używać jako id email lub numeru PESEL.

scope (string): określenie jakie dane mają być zwrócone partnerowi po weryfikacji tożsamości. Użytkownik otrzymuje informację, jakie dane zostaną a jakie nie zostaną zwrócone partnerowi. Można użyć następujących liter:

- f Imię
- l Nazwisko
- s Płeć
- b Data urodzenia (z dokładnością do miesięcy)
- h Hash numeru PESEL
- p Niezaszyfrowany numer PESEL

Opcja niezaszyfrowanego PESEL jest niedostępna bez indywidualnej umowy.



Weryfikacja tożsamości przez użytkownika

Użytkownik wykonuje standardowy proces potwierdzenia tożsamości poprzez podpisanie dokumentu i zwrócenie go do weryfikacji.

Przykładowa strona weryfikacji wywołana na żądanie ze strony partnera:

<https://www.gdziepolek.pl/weryfikacja-tozsamosci?partner=goldenberry&id=123&scope=flb>

Weryfikacja tożsamości

na podstawie Profilu Zaufanego

Strona **www.goldenberry.eu** chce zweryfikować Twoją tożsamość.

Dane, które zostaną jej przekazane, są oznaczone ✔:

- ✔ Fakt, że masz aktywny profil zaufany
- ✔ Imię
- ✔ Nazwisko
- ✘ Płeć
- ✔ Data urodzenia
- ✘ Zaszyfrowany bezpowrotnie PESEL

strona nie będzie mogła odszyfrować samego PESEL, ale jeśli sam jej go podasz, będzie mogła porównać, czy zgadza się z zaszyfrowanym

Podmiot odpowiedzialny za **www.goldenberry.eu** i administrator Twoich danych*:

Goldenberry sp. z o.o. sp. kom.
pl. Piłsudskiego 3, 00-095 Warszawa

Przekierowanie na stronę partnera

W przypadku zakończonej z sukcesem weryfikacji tożsamości użytkownik korzysta z odnośnika przekierowującego na stronę partnera.

Uwaga: przekierowanie może być ręcznie wywołane przez użytkownika, więc **nie należy** traktować go jako dowód pozytywnej weryfikacji, a jedynie informację, że można przystąpić do sprawdzenia wyniku.



URL partnera ma postać:

`https://domena-partnera/IdValidationCompleted`

Uwaga: wywołanie ma formę POST.

Jako parametr przekazywany jest:

id (string): przekazane przy wywołaniu usługi **Id operacji** sprawdzenia tożsamości przekazane przy wywołaniu usługi przez partnera.

Weryfikacja przez partnera wyniku sprawdzenia

Wynik sprawdzenia dostępny jest dla partnera przez okres godziny od załączenia podpisanego pliku przez użytkownika w trakcie weryfikacji (nie od powrotu na stronę partnera).

Aby sprawdzić wynik dla danego Id operacji należy wywołać URL:

`https://www.gdziepolek.pl/validate-id/check`

Wywołanie ma mieć formę **POST**.

Przekazywane parametry:

id (string): Id operacji

key (string): klucz API widoczny na widoku strony korzystającej z API po jej rejestracji

Przykład wywołania z linii terminala:

```
curl "https://www.gdziepolek.pl/validate-id/check" \
-X "POST" \
-d "id=rthsrthsrthw&partner=goldenberry&key=rth4343weferg"
```

Sprawdzenie wyniku weryfikacji powinno mieć miejsce tylko po stronie serwera, aby klucz dla API pozostał tajemnicą.

W przypadku dostępności wyniku zwracany jest JSON. Wypełnione są pola zgodnie z przekazanym zakresem weryfikacji tożsamości.



Przykład zwróconego JSON:

```
{"HasProfile":true,"FirstName":"JAN","LastName":"NOWAK","Sex":null,"PeselHash":null,"Pesel":null,"Birthdate":"1979-04-20"}
```

Hash PESEL to **SHA256** wywoływany na łańcuchu znaków w formie:

```
PESEL-IDPARTNERA
```

Na przykład dla partnera o Id **goldenberry** i PESEL **83030719694** będzie to odpowiednio:

```
83030719694-goldenberry
```

```
ff6fbd7749b670387cf47a4d766554f3a58ea2cfc41f2235fa26571929d2eacd
```




3. Opcjonalne dodatkowe usługi komercyjne

Proces korzystania z API oraz rejestracji korzystającej z niego strony jest samoobsługowy i bezpłatny, a usługa świadczona jest niekomercyjnie niezależnie od wolumenu.

Inne działania angażujące czas zespołu GdziePoLek są płatne. Wszystkie ceny netto.

Podpisanie indywidualnej standardowej umowy

Zmienione mogą być tylko dane podmiotu, umowa pozwala na kontynuację działania niezależnie do konta indywidualnego użytkownika. Zawiera 3-miesięczny okres wypowiedzenia.

10 000 zł

Rozpatrywanie propozycji zmian standardowej umowy

Przez okres 30 dni od wpłaty, obejmuje kontakty z działem prawnym lub innymi specjalistami. Nie zobowiązuje GdziePoLek do akceptacji żadnych zmian.

10 000 zł

Ustalenie i podpisanie NDA

Standardowa umowa gwarantuje tajemnicę danych weryfikowanych użytkowników, których GdziePoLek nie przechowuje, ale partner może mieć potrzebę przekazania GdziePoLek innych poufnych informacji (np. domena nowego produktu).

10 000 zł

**Uczestnictwo w formalnych procesach zakupowych**

Obejmuje takie czynności przez okres 30 dni od wpłaty jak wysłanie formalnej oferty w formie elektronicznej, rejestrację na portalu dostawców, kontakty z działem zakupów. Nie zobowiązuje GdziePoLek do jakichkolwiek zmian oferty.

10 000 zł

Dostosowanie produktu do specjalnych potrzeb partnera

Na przykład umieszczenie logo partnera na stronie weryfikacji, zmiana innych elementów wizualnych strony, przekierowanie na URL w innej domenie po zakończeniu weryfikacji, inicjowanie weryfikacji z wielu domen itp.

Od 2 000 zł miesięcznie



4. Regulamin (wersja robocza)

Wstęp

1. Niniejszy Regulamin określa zasady i warunki korzystania z interfejsu programistycznego aplikacji udostępnianego na stronie internetowej <https://www.gdziepolek.pl/weryfikacja-tozsamosci> („API”) oraz danych przesyłanych za pośrednictwem API („Dane”).
2. Podmiotem świadczącym usługi określone w Regulaminie jest **GdziePoLek spółka z ograniczoną odpowiedzialnością** z siedzibą w Warszawie przy pl. Piłsudskiego 3, kod pocztowy 00-078, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000530013, NIP 525-259-99-96, REGON 360126624 (dalej: „**GdziePoLek**”).

Definicje

Partner - oznacza osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, lecz posiadający na mocy ustawy zdolność prawną podmiot, który korzysta z API w celu w pozyskiwania danych identyfikujących osoby fizyczne, w szczególności w celu uwierzytelnienia Użytkownika.

Profil Zaufany – bezpłatna metoda potwierdzania tożsamości obywatela w ramach Elektronicznej Platformy Usług Administracji Publicznej (ePUAP).

Użytkownik – osoba fizyczna, będąca konsumentem, która chce potwierdzić tożsamość w celu realizacji operacji w serwisie Partnera.

Uwierzytelnianie - proces elektroniczny, który umożliwia identyfikację elektroniczną Użytkownika lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej. W API stosuje się czynniki uwierzytelnienia pochodzące z Elektronicznej Platformy Usług Administracji Publicznej (ePUAP).

Klucz API – unikalny identyfikator przyznawany w ramach dostępu do API, uzyskiwanego w procesie rejestracji konta na GdziePoLek.pl.

Umowa - umowa o korzystanie z API zawarta przez GdziePoLek z Partnerem na podstawie niniejszego Regulaminu.

Regulamin – niniejszy Regulamin korzystania z API.

Zawarcie Umowy

1. Umowa zostaje zawarta z chwilą rejestracji konta przez Partnera na portalu GdziePoLek.pl w celu korzystania z API.
2. Umowa zawarta jest na czas nieoznaczony.



3. Korzystanie przez Partnera z API na podstawie niniejszej Umowy jest nieodpłatne.
4. Dodatkowe działania angażujące czas zespołu GdziePoLek są odpłatne, w szczególności:
 - Podpisanie indywidualnej standardowej umowy
 - Rozpatrywanie propozycji zmian standardowej umowy
 - Uzgodnienie i podpisanie NDA
 - Uczestnictwo w formalnych procesach zakupowych
 - Dostosowanie usługi do indywidualnych potrzeb Partnera.

Cel

GdziePoLek stworzył API umożliwiające dostęp do procesu weryfikacji tożsamości Użytkownika przy wykorzystaniu Profilu Zaufanego, w celu umożliwienia uwierzytelnienia Użytkowników do świadczonych przez Partnera usług.

Zasady udostępniania i korzystania z API

1. Skorzystanie z API przez Partnera wymaga rejestracji konta na GdziePoLek.pl polegającej na podaniu pełnych i prawdziwych informacji oraz uzyskania klucza API.
2. GdziePoLek zastrzega sobie prawo do odmowy rejestracji lub przyznania Klucza API według własnego uznania.
3. Partner zobowiązuje się wykorzystywać API, zgodnie z prawem, jedynie w celu w jakim został on stworzony.
4. Partner nie jest w szczególności uprawniony do wykorzystywania API i Danych w związku z produktami lub usługami lub materiałami, które promują lub są wykorzystywane w celach związanych z: oprogramowaniem szpiegującym, przechwytywaniem danych, hazardem, nielegalnym gromadzeniem i przetwarzaniem danych osobowych oraz materiałami propagującymi przemoc i rasizm.
5. GdziePoLek ma prawo do zablokowania Klucza API w przypadku, gdy:
 - a. Partner w ocenie GdziePoLek nie daje należytej rękojmi rzetelnego postępowania zgodnie z przepisami niniejszego Regulaminu,
 - b. Partner korzystając z API narusza niniejszy Regulamin,
 - c. Partner korzystając z API narusza powszechnie obowiązujące przepisy prawa bądź w inny sposób może naruszać interesy GdziePoLek bądź jej klientów i kontrahentów.
6. Partner zobowiązuje się nie udostępniać Klucza API osobom trzecim i ponosi wszelką odpowiedzialność za jego wykorzystanie w celach sprzecznych z obowiązującym prawem, dobrymi obyczajami oraz niniejszym Regulaminem. Odpowiedzialność Partnera rozciąga się również na działanie osób, którym Klucz API został udostępniony, nawet w sposób niezawiniony.



7. GdziePoLek zastrzega sobie możliwość wprowadzania przerw technicznych w funkcjonowaniu API w przypadku prowadzenia prac technicznych dotyczących funkcjonowania API, przy czym stosowne informacje o pracach technicznych będą przekazywane przez GdziePoLek komunikatami zamieszczanymi w API lub na podany przez Partnera adres e-mail.
8. GdziePoLek zastrzega sobie możliwość wprowadzania dowolnych zmian w API, w tym w szczególności dotyczących wprowadzania nowych usług i rozszerzania funkcjonalności w ramach API lub zaprzestania świadczenia określonych usług oraz wyłączania określonych funkcjonalności API zgodnie z obowiązującymi przepisami prawa.
9. GdziePoLek nie gwarantuje, jak również nie składa jakichkolwiek oświadczeń co do funkcjonalności API, braku ewentualnych błędów w ramach API oraz występowania w ramach API jakichkolwiek braków. Wszelka odpowiedzialność GdziePoLek w tym zakresie jest wyłączona w zakresie dopuszczonym przez obowiązujące przepisy.

Dane osobowe

1. GdziePoLek informuje, że administratorem danych osobowych przetwarzanych w celu potwierdzenia tożsamości Użytkownika jest Partner.
2. GdziePoLek nie przechowuje danych osobowych przekazanych w celu potwierdzenia tożsamości Użytkownika.
3. Informacjami zawartymi w profilu użytkownika ePUAP administruje podmiot wskazany przez dysponenta ePUAP, tj. ministra ds. informatyzacji.

Zmiany Regulaminu

1. GdziePoLek zastrzega sobie prawo do zmiany postanowień Regulaminu w dowolnym momencie.
2. W przypadku, gdy w ocenie GdziePoLek modyfikacja może mieć negatywny wpływ na Partnera, GdziePoLek powiadomi o tym Partnera z siedmiodniowym wyprzedzeniem korzystając z adresu e-mail Partnera podanego podczas procesu rejestracji.
3. W przypadku, gdy Partner nie akceptuje wprowadzonych do Regulaminu zmian, jest zobowiązany do wypowiedzenia Umowy poprzez zaprzestanie korzystania z API w terminie do 7 dni od otrzymania powiadomienia.

Rozwiązanie umowy

1. GdziePoLek zastrzega sobie prawo, według własnego uznania i w dowolnym czasie bez powiadomienia, do zmiany, zawieszenia lub przerwania dostępu do interfejsu API lub wypowiedzenia Umowy.
2. Po każdym rozwiązaniu Umowy Partner niezwłocznie usunie wszystkie wywołania API ze wszystkich stron internetowych, skryptów, widżetów, aplikacji i innego oprogramowania będącego w posiadaniu lub pod kontrolą Partnera.



3. Partner może w każdym czasie wypowiedzieć niniejszą umowę, dotyczącą wskazanego przez niego Klucza API przypisanego mu w ramach jego konta poprzez zgłoszenie na adres: kontakt@gdziepolek.pl.

Postanowienia końcowe

1. Niniejszy Regulamin dostępny jest pod adresem internetowym:
https://gdziepolek.blob.core.windows.net/cdn/static/GdziePoLek_Weryfikacja_Toz%CC%87samos%CC%81ci_v1.pdf
2. Prawem właściwym dla Umowy jest prawo obowiązujące w Polsce.
3. Korespondencję elektroniczną dotyczącą API można kierować na adres e-mail: kontakt@gdziepolek.pl.