

Regulamin Serwisu ScoreUp.pl

§ 1 Postanowienia Ogólne

1. Niniejszy Regulamin określa zasady i warunki świadczenia usług drogą elektroniczną przez Usługodawcę za pośrednictwem serwisu internetowego działającego pod domeną **ScoreUp.pl**, skierowane zarówno do Klientów, jak i do Partnerów.
2. Właścicielem Serwisu i Usługodawcą jest: **ScoreUp Spółka z Ograniczoną Odpowiedzialnością** z siedzibą w Krakowie przy ul. Karmelickiej 32/20, 31-128 Kraków, (dalej: „Usługodawca” lub „ScoreUp”).
3. Kontakt z Usługodawcą możliwy jest pod adresem e-mail: kontakt@scoreup.pl.
4. Przedmiotem działalności Serwisu jest świadczenie usług analizy raportów kredytowych (BIK) oraz dostarczanie narzędzi i dokumentacji służących optymalizacji historii kredytowej, a także pośrednictwo w udostępnianiu ofert usług podmiotów partnerskich.

§ 2 Definicje

Użyte w Regulaminie pojęcia oznaczają:

1. **BIK** – Biuro Informacji Kredytowej S.A., oznacza instytucję działającą w Polsce, której głównym zadaniem jest gromadzenie, przechowywanie i udostępnianie informacji o historii kredytowej klientów indywidualnych oraz firm.
2. **Kancelaria** – podmiot partnerski świadczący profesjonalne usługi prawne: CREO Kancelaria Prawna sp. z o.o. z siedzibą w Krakowie.
3. **Klient** – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której Raport BIK poddawany jest analizie i na rzecz której świadczona jest Usługa za pośrednictwem Partnera.
4. **Partner** – podmiot współpracujący z Usługodawcą, posiadający dostęp do systemu partnerskiego ScoreUp, działający jako pośrednik techniczny wspierający Klienta w procesie składania zamówienia i obsługi Serwisu.
5. **Raport BIK** – raport zawierający historię kredytową Klienta, pobrany z Biura Informacji Kredytowej S.A.
6. **Regulamin** – niniejszy Regulamin określony przez Usługodawcę, który precyzuje warunki świadczenia usług w rozumieniu przepisów Ustawy.
7. **Serwis** – serwis internetowy Usługodawcy znajdujący się pod adresem <http://www.scoreup.pl>.
8. **Umowa** – umowa zawierana pomiędzy Usługodawcą a Klientem za pośrednictwem Serwisu, na podstawie której Usługodawca zobowiązuje się do świadczenia Usług na rzecz Klienta.
9. **Umowa Partnerska** – umowa o współpracę zawarta pomiędzy Usługodawcą a Partnerem.
10. **Umowa Powierzenia (DPA)** – umowa regulująca zasady przetwarzania danych osobowych przez ScoreUp na zlecenie Partnera, stanowiąca Załącznik nr 1 do niniejszego Regulaminu i stanowiąca jego integralną część.
11. **Usługa** – usługi świadczone drogą elektroniczną przez ScoreUp zgodnie z § 4 Regulaminu.

§ 3 Warunki świadczenia Usług

1. Klient jest świadomy i akceptuje, że Usługi oferowane przez Usługodawcę polegają na przygotowaniu personalizowanej dokumentacji umożliwiającej natychmiastowe samodzielnie rozpoczęcie procesu optymalizacji Raportu BIK przez Klienta albo zaoferowaniu Klientowi skorzystania z usług partnerskiej Kancelarii.
2. Dokonywanie zamówień w imieniu i na rzecz Klienta możliwe jest za pośrednictwem Partnera, z którym Usługodawca posiada zawartą Umowę Partnerską oraz wyłącznie po przekazaniu Partnerowi przez Klienta Raportu BIK Klienta mającego być przedmiotem analizy w Serwisie.
3. W celu skorzystania z Usługi, niezbędne jest zalogowanie się Partnera do Serwisu, przesłanie do analizy Raportu BIK Klienta oraz wybór odpowiedniego rozwiązania z oferty Usługodawcy.
4. Aby skorzystać z Usług, Klient musi prawidłowo umocować Partnera do działania w jego imieniu i na jego rzecz oraz wyrazić wymagane przepisami prawa zgody.
5. Partner zobowiązuje się do utrzymania w poufności danych dostępowych do Serwisu i nieudostępniania konta osobom nieupoważnionym. Partner ponosi pełną odpowiedzialność za działania osób, którym faktycznie umożliwił dostęp do Serwisu.

§ 4 Model świadczenia usług

1. **Analiza i Rekomendacja (Usługa Diagnostyczna)** - podstawowa Usługa świadczona przez Usługodawcę polega na automatycznej analizie dostarczonego Raportu BIK Klienta. W jej wyniku system generuje wykaz pozycji (wpisów w BIK), które kwalifikują się do podjęcia działań optymalizacyjnych, wraz z oceną zasadności takich działań, oraz identyfikuje potencjalne możliwości skorzystania z produktów dodatkowych (np. zwrot prowizji).
2. **Decyzja o zakresie Usługi** - na podstawie wyników analizy, o której mowa w ust. 1, Klient - przy wsparciu Partnera - podejmuje decyzję o zakresie zamawianej Usługi. Decyzja ta obejmuje wybór konkretnych pozycji z Raportu BIK, dla których ma zostać wygenerowana spersonalizowana dokumentacja („Optymalizacja”), lub wybór produktów dodatkowych realizowanych przez Kancelarię.
3. **Realizacja Optymalizacji** - w przypadku wybrania przez Klienta wariantu Optymalizacji dla wskazanych pozycji, Usługa polega na wygenerowaniu i udostępnieniu Klientowi spersonalizowanych wzorów pism i dokumentów niezbędnych do samodzielnego przeprowadzenia procedury usunięcia lub korekty danych w BIK.
4. **Produkty Kancelarii (Usługi Prawne)** - w przypadku, gdy system zidentyfikuje możliwość realizacji usług prawnych (np. sankcja kredytowa pro, zaawansowane czyszczenie BIK) i Klient wyrazi wolę skorzystania z tej opcji poprzez zaznaczenie odpowiedniego wyboru w systemie:
 - a) Rola ScoreUp ogranicza się do przekazania Klientowi informacji o ofercie oraz przekazania danych Klienta do Kancelarii w celu przygotowania umowy;
 - b) Usługi te są świadczone bezpośrednio przez Kancelarię na podstawie odrębnej umowy zawieranej między Klientem a Kancelarią;
 - c) ScoreUp nie jest stroną umowy o świadczenie usług prawnych i nie ponosi odpowiedzialności za działania Kancelarii.
5. **Rola Partnera i Złożenie Dyspozycji** - Partner działa w procesie jako pośrednik techniczny. Po ustaleniu z Klientem zakresu Usług (wybór pozycji do optymalizacji lub produktów Kancelarii), Partner wprowadza dane Klienta oraz wybrane parametry zamówienia do systemu teleinformatycznego Serwisu. Czynność ta stanowi techniczne przygotowanie zamówienia i nie jest równoznaczna z zawarciem Umowy.

6. **Procedura Zawarcia Umowy** Do zawarcia Umowy o świadczenie Usług pomiędzy Usługodawcą (ScoreUp) a Klientem dochodzi w trybie ofertowym, zgodnie z następującą procedurą:
- Po wprowadzeniu danych przez Partnera, system automatycznie generuje i wysyła na adres e-mail Klienta wiadomość zawierającą indywidualny link do Regulaminu z możliwością jego akceptacji (przycisk po przejściu na stronę pod linkiem „Akceptuję Regulamin” wraz z pełnym regulaminem do wglądu).
 - Po akceptacji Regulaminu przez Klienta, Klient otrzymuje drugą wiadomość e-mail zawierającą podsumowanie zamówienia wraz z informacjami jak dokonać płatności.
 - Klient weryfikuje treść zamówienia i jeśli je akceptuje, dokonuje płatności za zamówienie.
 - Do zawarcia Umowy dochodzi wyłącznie w momencie łącznego spełnienia dwóch warunków: akceptacji Regulaminu (dokonanej poprzez kliknięcie w link akceptacyjny) oraz potwierdzenia warunków zamówienia poprzez dokonanie płatności.
 - Brak akceptacji lub brak płatności w terminie wskazanym w wiadomości (lub w przypadku braku terminu – 7 dni) powoduje anulowanie dyspozycji wprowadzonej przez Partnera. W takim przypadku Umowa nie zostaje zawarta, a Usługodawca nie pobiera żadnych opłat.

§ 5 Płatności

- Usługi świadczone przez ScoreUp są odpłatne zgodnie z Cennikiem obowiązującym w dniu złożenia zamówienia. Informacja o całkowitym koszcie Usługi jest przedstawiana Klientowi (za pośrednictwem Partnera) przed finalizacją zamówienia oraz potwierdzona w wiadomości e-mail.
- Usługi oferowane przez Usługodawcę są płatne, a wynagrodzenie za nie jest uiszczane przez Klienta.
- Dokonanie płatności jest warunkiem koniecznym do prawidłowego wykonania Usługi przez Usługodawcę i warunkuje otrzymanie przez Klienta dopasowanych rekomendacji dotyczących możliwości i sposobów optymalizacji danych Klienta w BIK.
- Płatność za Usługi ScoreUp (analiza, dokumentacja optymalizacyjna) dokonywana jest za pośrednictwem operatora płatności (np. TPay) lub przelewem tradycyjnym.
- W przypadku wyboru produktów realizowanych przez Kancelarię, wynagrodzenie z tego tytułu jest należne wyłącznie Kancelarii i rozliczane na podstawie umowy zawartej bezpośrednio z Kancelarią. ScoreUp nie pobiera opłat z tytułu usług prawnych świadczonych przez Kancelarię.

§ 6 Odpowiedzialność i Gwarancje

- Usługodawca dokłada wszelkich starań, aby generowana dokumentacja była zgodna z aktualnym stanem prawnym i najwyższymi standardami rynkowymi.
- Usługodawca nie ponosi odpowiedzialności za prawidłowość danych Klienta zawartych w Raporcie BIK przekazanym przez Partnera.

3. Usługodawca informuje, że ostateczna decyzja o usunięciu wpisu z bazy BIK lub zwrocie prowizji należy do instytucji finansowej (banku, firmy pożyczkowej). W związku z tym Usługodawca **nie gwarantuje** osiągnięcia zamierzonego przez Klienta skutku (np. usunięcia wpisu, podniesienia punktacji scoringowej) i nie ponosi odpowiedzialności za odmowne decyzje instytucji finansowych.
4. Odpowiedzialność Usługodawcy względem Klienta ograniczona jest do wysokości rzeczywiście poniesionej straty i nie obejmuje utraconych korzyści.
5. Usługodawca nie gwarantuje skuteczności działań podejmowanych przez Kancelarię.
6. Usługi nie mogą być wykorzystane w celu dalszej odsprzedaży lub nieodpłatnego udostępnienia innym Klientom, co oznacza, że Usługi mogą być świadczone wyłącznie na rzecz i na indywidualny użytek danego Klienta.

§ 7 Odstąpienie od Umowy

1. Klientowi będącemu konsumentem przysługuje prawo do odstąpienia od Umowy w terminie 14 dni bez podania przyczyny.
2. Prawo do odstąpienia od Umowy **nie przysługuje** w odniesieniu do umów o dostarczanie treści cyfrowych niedostarczonych na nośniku materialnym (np. wygenerowane dokumenty PDF, raport z analizy), jeżeli spełnianie świadczenia rozpoczęło się za wyraźną i uprzednią zgodą Klienta przed upływem terminu do odstąpienia od Umowy i po poinformowaniu go o utracie prawa odstąpienia od umowy.
3. Poprzez akceptację Regulaminu i dokonanie płatności, Klient wyraża wyraźną zgodę na rozpoczęcie świadczenia Usługi przed upływem terminu do odstąpienia od Umowy i przyjmuje do wiadomości, że z chwilą dostarczenia mu gotowej analizy lub dokumentacji traci prawo do odstąpienia od Umowy.

§ 8 Reklamacje

1. Klient ma prawo składać reklamacje dotyczące działania Serwisu oraz jakości świadczonych Usług na adres e-mail: kontakt@scoreup.pl.
2. Reklamacja powinna zawierać dane identyfikacyjne Klienta oraz opis zgłaszanych zastrzeżeń.
3. Usługodawca rozpatruje reklamację w terminie 14 dni od daty jej otrzymania.
4. Reklamacje dotyczące usług prawnych świadczonych przez Kancelarię należy kierować bezpośrednio do Kancelarii.
5. W przypadku, gdy złożona reklamacja zawiera braki uniemożliwiające jej rozpatrzenie, Usługodawca może wezwać do jej uzupełnienia, określając termin i zakres tego uzupełnienia z pouczeniem, że nieuzupełnienie reklamacji w określonym terminie spowoduje pozostawienie reklamacji bez rozpoznania.
6. Po bezskutecznym upływie wyznaczonego terminu reklamację pozostawia się bez rozpoznania.
7. Odpowiedź na reklamację Usługodawca kieruje na adres poczty elektronicznej wskazany w treści reklamacji lub pisemnie na adres nadawcy.

§ 9 Wymagania Techniczne

1. Prawidłowe korzystanie z Usług świadczonych za pośrednictwem Serwisu wymaga:
 - a) połączenia z siecią Internet,
 - b) zainstalowania najnowszej wersji przeglądarki internetowej umożliwiającej wyświetlanie na ekranie komputera dokumentów hipertekstowych (HTML),
 - c) włączonej obsługi plików cookies oraz JavaScript,
 - d) braku zainstalowanych wtyczek lub rozszerzeń w przeglądarce internetowej ingerujących w treść strony internetowej,
 - e) posiadania konta poczty elektronicznej;
2. Usługodawca nie ponosi odpowiedzialności za odpowiedni stan techniczny lub właściwą

konfigurację sprzętu używanego w celu skorzystania z Usług.

3. Usługodawca nie ponosi odpowiedzialności za przerwy w świadczeniu Usług wynikające z awarii lub przypadków wadliwego funkcjonowania systemów teleinformatycznych będących poza jego wpływem lub kontrolą.

§ 10 Ochrona Danych Osobowych (RODO)

1. W odniesieniu do czynności realizowanych na podstawie § 3 ust. 2–3 oraz § 4 ust. 1 i 5 niniejszego Regulaminu administratorem danych osobowych Klienta jest Partner. Usługodawca przetwarza te dane jako Podmiot Przetwarzający (procesor) na udokumentowane zlecenie Partnera, na warunkach szczegółowo opisanych w Umowie Powierzenia, stanowiącej **Załącznik nr 1** do niniejszego Regulaminu. Akceptując Regulamin, Partner oświadcza i gwarantuje, że posiada wszelkie wymagane prawem, udokumentowane zgody i upoważnienia Klienta na pozyskanie jego Raportu BIK oraz wprowadzenie go do systemów Serwisu.
2. Z momentem skutecznego zawarcia Umowy o świadczenie Usług pomiędzy Usługodawcą a Klientem Usługodawca staje się samodzielnym administratorem danych osobowych Klienta w rozumieniu art. 4 pkt 7 RODO. Akceptując niniejszy Regulamin, Klient przyjmuje do wiadomości, że jego dane osobowe będą przetwarzane przez Usługodawcę jako samodzielnego administratora danych osobowych.
3. Szczegółowa informacja dotycząca przetwarzania danych osobowych przez Usługodawcę znajduje się w Polityce Prywatności Serwisu.

§ 11 Postanowienia Końcowe

1. Regulamin wchodzi w życie z dniem 15.06.2026 r.
2. Usługodawca zastrzega sobie prawo do zmiany Regulaminu. Zmiany wchodzi w życie z chwilą ich opublikowania w Serwisie, przy czym do zamówień złożonych przed zmianą stosuje się przepisy dotychczasowe.
3. W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie mają przepisy prawa polskiego, w szczególności Kodeksu cywilnego oraz Ustawy o prawach konsumenta.
4. Integralną część niniejszego Regulaminu stanowią załączniki:
Załącznik nr 1 – Umowa Powierzenia.

**UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
(„UMOWA POWIERZENIA”)**

Umowa Powierzenia stanowi integralną część Regulaminu i określa zasady przetwarzania przez Usługodawcę na zlecenie Partnera danych osobowych Klientów za pośrednictwem Serwisu zgodnie z art. 28 RODO.

§ 1. Definicje

1. **Administrator Danych** – oznacza Partnera, który samodzielnie ustala cele i sposoby przetwarzania Danych Osobowych.
2. **Cel Przetwarzania** – oznacza realizację przez Podmiot Przetwarzający automatycznej analizy kredytowej Raportu BIK w celu wskazania pozycji kwalifikujących się do optymalizacji.
3. **Czynności Przetwarzania** – oznaczają wszelkie operacje na Danych Osobowych, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, ograniczanie, usuwanie lub niszczenie.
4. **Dalszy Podmiot Przetwarzający (DPP)** – oznacza podmiot, z którego usług korzysta Podmiot Przetwarzający przy wykonywaniu umowy i dokonywaniu konkretnych Czynności Przetwarzania, który będzie miał dostęp do Danych Osobowych.
5. **Dane Osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, których dotyczy powierzenie, a których szczegółowy zakres określa **Załącznik nr 1** do niniejszej Umowy.
6. **EOG** – oznacza Europejski Obszar Gospodarczy.
7. **Kontrola Przetwarzania** – oznacza audyty (w tym inspekcje) zgodności przetwarzania Danych Osobowych w Serwisie z przepisami prawa oraz niniejszą Umową Powierzenia.
8. **Naruszenie Ochrony Danych Osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do powierzonych Danych Osobowych.
9. **Ocena Skutków dla Ochrony Danych** – ocena skutków planowanych operacji przetwarzania, o której mowa w art. 35 RODO.
10. **Organ Nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych lub inny właściwy organ nadzorczy w rozumieniu art. 4 pkt 21 RODO.
11. **Podmiot Przetwarzający** – oznacza Usługodawcę, który przetwarza Dane Osobowe na wyraźne polecenie Administratora Danych w związku z realizacją Usług.
12. **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
13. **Standardowe Klauzule Umowne** – standardowe klauzule ochrony danych przyjęte przez Komisję Europejską, o których mowa w art. 46 RODO.

§ 2. Przedmiot i czas trwania przetwarzania

1. Administrator Danych powierza Podmiotowi Przetwarzającemu przetwarzanie Danych Osobowych w celu realizacji usługi automatycznej analizy Raportów BIK, a Podmiot Przetwarzający to zlecenie przyjmuje.
2. Zawarcie niniejszej Umowy Powierzenia stanowi udokumentowane polecenie Administratora Danych do przetwarzania Danych Osobowych przez Podmiot Przetwarzający.

§ 3. Środki techniczne i organizacyjne

1. Podmiot Przetwarzający zapewnia środki techniczne i organizacyjne adekwatne do rodzaju Danych Osobowych oraz ryzyka naruszenia praw lub wolności osób, których dane dotyczą, zgodnie z art. 32 RODO.
2. Szczegółowa lista minimalnych środków technicznych i organizacyjnych stanowi **Załącznik nr 2** do niniejszej Umowy. Podmiot Przetwarzający może zmieniać lub wprowadzać inne środki techniczne i organizacyjne, pod warunkiem że będą spełniały wymogi określone w ust. 1 powyżej.

§ 4. Personel Podmiotu Przetwarzającego

1. Podmiot Przetwarzający dopuści do przetwarzania Danych Osobowych jedynie osoby działające z jego upoważnienia, których dostęp do danych jest niezbędny do prawidłowego wykonania Usługi.
2. Podmiot Przetwarzający zapewni, aby osoby upoważnione zobowiązały się do zachowania tajemnicy przetwarzanych Danych Osobowych lub podlegały ustawowemu obowiązkowi zachowania tajemnicy.

§ 5. Dalsze Podmioty Przetwarzające

1. Administrator Danych wyraża ogólną zgodę na korzystanie przez Podmiot Przetwarzający z usług Dalszych Podmiotów Przetwarzających w celu prawidłowego świadczenia Usług i bezpieczeństwa Serwisu.
2. Lista Dalszych Podmiotów Przetwarzających, z których Podmiot Przetwarzający korzysta na dzień rozpoczęcia obowiązywania Umowy, stanowi **Załącznik nr 3** do niniejszej Umowy. Administrator Danych zawierając Umowę Powierzenia, akceptuje powierzenie przetwarzania Danych Osobowych podmiotom wskazanym w **Załączniku nr 3**.
3. W przypadku zamiaru skorzystania z usług innych Dalszych Podmiotów Przetwarzających, Podmiot Przetwarzający prześle Administratorowi Danych informację w postaci elektronicznej co najmniej na 30 dni przed dokonaniem dalszego powierzenia. Zmiana **Załącznika nr 3** nie wymaga zmiany niniejszej Umowy Powierzenia.
4. Administrator Danych może zgłosić umotywowany sprzeciw wobec nowego Dalszego Podmiotu Przetwarzającego w terminie 14 dni od otrzymania informacji, o której mowa w ust. 3 powyżej. Zgłoszenie sprzeciwu uprawnia Administratora Danych do wypowiedzenia umowy z Podmiotem Przetwarzającym ze skutkiem na koniec miesiąca następującego po miesiącu, w którym złożono sprzeciw.
5. Podmiot Przetwarzający nakłada na Dalszy Podmiot Przetwarzający w drodze umowy te same obowiązki ochrony danych, jakie wynikają z niniejszej Umowy Powierzenia.

6. Podmiot Przetwarzający ponosi odpowiedzialność za działania i zaniechania Dalszych Podmiotów Przetwarzających jak za własne działania i zaniechania.

§ 6. Transfer danych poza Europejski Obszar Gospodarczy (EOG)

1. W przypadku zamiaru powierzenia przetwarzania Danych Osobowych Dalszemu Podmiotowi Przetwarzającemu, które wymagałoby przekazywania danych do państw trzecich (poza EOG), stosuje się odpowiednio procedurę informowania i zgłaszania sprzeciwu określoną w § 5 niniejszej Umowy Powierzenia, z tym że informacja o nowym Dalszym Podmiocie Przetwarzającym zawierać będzie dodatkowo informacje o:
 - a) podstawach prawnych transferu (w szczególności: decyzja Komisji Europejskiej o odpowiednim stopniu ochrony, Standardowe Klauzule Umowne lub inne odpowiednie zabezpieczenia zgodnie z art. 46 RODO);
 - b) środkach dodatkowych stosowanych w celu zapewnienia odpowiedniego stopnia ochrony Danych Osobowych.
2. W przypadku zgłoszenia przez Administratora Danych uzasadnionego sprzeciwu wobec nowego Dalszego Podmiotu Przetwarzającego mającego siedzibę poza EOG, Podmiot Przetwarzający nie jest uprawniony do przekazywania powierzonych Danych Osobowych temu podmiotowi.

§ 7. Pomoc dla Administratora Danych

1. Uwzględniając charakter Czynności Przetwarzania, Podmiot Przetwarzający zapewni Administratorowi Danych pomoc w wywiązaniu się z obowiązków:
 - a) wsparcia w realizacji praw osób, których dane dotyczą (art. 15–22 RODO). W przypadku otrzymania przez Podmiot Przetwarzający żądania bezpośrednio od osoby, której dane dotyczą, Podmiot Przetwarzający niezwłocznie poinformuje o tym Administratora Danych.
 - b) zgłaszania Naruszenia Ochrony Danych Osobowych Organowi Nadzorcemu oraz zawiadamiania osób, których dane dotyczą (art. 33-34 RODO).
 - c) przeprowadzenia Oceny Skutków dla Ochrony Danych (art. 35 RODO) poprzez udzielanie niezbędnych informacji dotyczących działania Usługi.
2. Na żądanie Administratora Danych Podmiot Przetwarzający udostępni wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§ 8. Naruszenie Ochrony Danych Osobowych

1. W przypadku stwierdzenia Naruszenia Ochrony Danych Osobowych, Podmiot Przetwarzający zgłosi je Administratorowi Danych niezwłocznie, nie później niż w terminie 36 godzin od jego stwierdzenia.
2. Zgłoszenie naruszenia będzie zawierać: opis okoliczności naruszenia, kategorie i przybliżoną liczbę osób/wpisów, których dotyczy naruszenie, możliwe konsekwencje oraz zastosowane środki zaradcze.
3. Podmiot Przetwarzający podejmuje niezwłocznie wszelkie niezbędne środki w celu zminimalizowania negatywnych konsekwencji naruszenia.
4. Podmiot Przetwarzający dokumentuje wszelkie Naruszenia Ochrony Danych Osobowych, w tym okoliczności, skutki i podjęte działania zaradcze, zgodnie z art. 33 ust. 5 RODO.

§ 9. Kontrola Przetwarzania

1. Administrator Danych jest uprawniony do przeprowadzenia Kontroli Przetwarzania Danych Osobowych przez Podmiot Przetwarzający z niniejszą Umową Powierzenia oraz przepisami prawa, w szczególności z RODO w każdym czasie, po zawiadomieniu Podmiotu Przetwarzającego co najmniej na 10 Dni Roboczych przed planowaną datą rozpoczęcia Kontroli Przetwarzania. Zawiadomienie powinno wskazywać: zakres kontroli, planowany termin oraz dane osób upoważnionych do jej przeprowadzenia.
2. Administrator Danych nie ponosi opłat za Kontrolę Przetwarzania, jeśli: (i) obowiązek jej przeprowadzenia został nałożony przez Organ Nadzorczy lub (ii) Kontrola Przetwarzania jest konieczna dla wyjaśnienia zaistniałego Naruszenia Ochrony Danych Osobowych.
3. W pozostałych przypadkach Podmiot Przetwarzający jest uprawniony do pobrania od Administratora Danych opłaty w celu pokrycia kosztów obsługi Kontroli Przetwarzania, zgodnie z cennikiem stanowiącym **Załącznik nr 4**.
4. Kontrola Przetwarzania nie może trwać dłużej niż 3 dni robocze, chyba że Strony uzgodnią inaczej.
5. Przed rozpoczęciem Kontroli Przetwarzania Podmiot Przetwarzający ma prawo żądać od Administratora Danych (oraz jego zewnętrznego audytora) zawarcia umowy o zachowaniu poufności (NDA).
6. Kontrola Przetwarzania zostaje zakończona podpisaniem przez obie Strony protokołu zawierającego wnioski z kontroli oraz uzgodniony zakres ewentualnych zmian.

§ 10. Zakończenie przetwarzania Danych Osobowych

1. Po zakończeniu świadczenia usług związanych z przetwarzaniem Danych Osobowych Podmiot Przetwarzający – zależnie od decyzji Administratora Danych - zwraca Administratorowi Danych wszelkie powierzone Dane Osobowe lub usuwa ich istniejące kopie, chyba że odpowiednie przepisy prawa nakazują przechowywanie tych Danych Osobowych.
2. Usunięcie Danych Osobowych z wszelkich nośników elektronicznych, w tym z baz danych oraz kopii zapasowych nastąpi nie później niż w terminie 30 dni od dnia zakończenia obowiązywania Umowy partnerskiej, chyba że Strony w drodze odrębnego porozumienia ustalą inny termin.
3. Strony zgodnie potwierdzają, że obowiązek usunięcia lub zwrotu danych, o którym mowa w ust. 1, nie obejmuje tych Danych Osobowych, w stosunku do których Podmiot Przetwarzający stał się samodzielnym administratorem danych osobowych na podstawie przepisów prawa i odrębnego stosunku prawnego. Dotyczy to w szczególności sytuacji, w których Klienci (w rozumieniu Regulaminu) samodzielnie zaakceptowali Regulamin i dokonali opłaty za realizację usług przez Podmiot Przetwarzający.
4. Podmiot Przetwarzający zobowiązuje się zapewnić, aby wszystkie Dalsze Podmioty Przetwarzające usunęły lub zanonimizowały Dane Osobowe na zasadach określonych w niniejszym paragrafie.

ZAŁĄCZNIK NR 1
ZAKRES DANYCH OSOBOWYCH

Kategoria osób, których dane dotyczą	Rodzaj danych osobowych	Czynności przetwarzania	Forma przetwarzania
Klienci Administratora Danych	Imię, nazwisko, adres e-mail, numer telefonu, numer PESEL lub NIP. Dane finansowe zawarte w Raporcie BIK, w szczególności: pełna historia kredytowa, statusy zobowiązań, zadłużenia, punktacja scoringowa.	Zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, przeglądanie, ujawnianie poprzez przesyłanie, usuwanie lub niszczenie.	Elektroniczna

ZAŁĄCZNIK NR 2

LISTA ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH

I. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Zabezpieczenia organizacyjne:

- **Procedury dostępu:** Podmiot Przetwarzający operacyjnie kontroluje procesy nadawania i odbierania uprawnień. Każdorazowe przyznanie dostępu do systemów produkcyjnych i wspierających wymaga weryfikacji oraz akceptacji administratora systemu, a działania te są rejestrowane w dziennikach zdarzeń. W przypadku zakończenia współpracy z personelem, dostępy i klucze dostępowe są niezwłocznie blokowane i usuwane.
- **Szkolenia personelu:** Osoby dopuszczone do przetwarzania danych przechodzą szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji oraz są zobowiązane do zachowania tajemnicy.
- **Zarządzanie incydentami:** Podmiot Przetwarzający posiada Procedurę zarządzania incydentami, wykorzystuje zautomatyzowane systemy do wykrywania zdarzeń sieciowych i aplikacyjnych oraz dedykowaną, centralną platformę zgłoszeniową umożliwiającą rejestrację, identyfikację oraz bieżącą obsługę zdarzeń związanych z bezpieczeństwem.

2. Zabezpieczenia dotyczące bezpieczeństwa fizycznego i modelu pracy:

- **Model pracy zdalnej:** Podmiot Przetwarzający działa w modelu pracy w pełni zdalnej i nie utrzymuje fizycznej infrastruktury biurowej ani własnych serwerowni. Dane nie są przechowywane lokalnie na urządzeniach końcowych zespołu.
- **Bezpieczeństwo Centrów Danych:** Infrastruktura produkcyjna hostowana jest wyłącznie w renomowanych centrach danych, które posiadają certyfikaty bezpieczeństwa fizycznego SOC 2 oraz ISO 27001.

3. Zabezpieczenia dotyczące kontroli dostępu:

- **Unikalne identyfikatory:** Każdy członek personelu posiada indywidualne, odrębne konto dostępowe do systemów informatycznych.
- **Dostęp do infrastruktury:** Dostęp do serwerów na platformie hostingowej realizowany jest wyłącznie za pomocą bezpiecznych protokołów komunikacyjnych przy użyciu indywidualnych, asymetrycznych kluczy kryptograficznych. Tradycyjny dostęp hasłowy do systemów bazodanowych i serwerów jest zablokowany.
- **Kontrola uprawnień (RBAC):** Wdrożono system kontroli dostępu oparty na rolach, ograniczający uprawnienia użytkowników wyłącznie do zasobów niezbędnych do wykonywania ich konkretnych zadań.

4. Zabezpieczenia dotyczące bezpieczeństwa operacyjnego:

- **Zarządzanie podatnościami:** Wdrożono zautomatyzowane, cotygodniowe skanowanie zależności kodu źródłowego i używanych bibliotek pod kątem znanych podatności, raportujące wykryte błędy bezpośrednio do kanałów monitoringu zespołu deweloperskiego.
- **Zarządzanie zmianą:** Proces wdrożeniowy oparty jest o profesjonalny system kontroli wersji z wymogiem procedury weryfikacji kodu (code review) oraz automatycznych testów jednostkowych i integracyjnych na odseparowanym środowisku testowym przed każdym wdrożeniem produkcyjnym.

- **Ochrona stacji roboczych:** Wszystkie urządzenia końcowe personelu posiadają aktywne i automatycznie aktualizowane oprogramowanie antywirusowe oraz systemowe zapory sieciowe. Wdrożono automatyczną blokadę ekranu po czasie nieaktywności.

II. BEZPIECZEŃSTWO SERWISU

Zabezpieczenia Serwisu zostały zaprojektowane i wdrożone w oparciu o architekturę wielowarstwową oraz standardy OWASP.

1. Zabezpieczenia sieciowe i strefy ochronne:

- **Wielowarstwowa ochrona sieci:** Na brzegu sieci wdrożono architekturę ochronną typu Web Application Firewall (WAF), zapewniającą aktywną ochronę przed atakami DDoS, rozproszoną sieć dostarczania treści (CDN) oraz bezpieczny, filtrowany system DNS.
- **Izolacja usług:** Komponenty systemu są izolowane na poziomie procesów wirtualnych przy użyciu restrykcyjnych reguł firewallu i wydzielonych portów komunikacyjnych. Środowisko produkcyjne jest całkowicie odseparowane sieciowo i zasobowo od środowiska testowego.

2. Szyfrowanie danych i mechanizmy kryptograficzne:

- **Szyfrowanie danych w spoczynku (Encryption at Rest):** Dane osobowe w bazie danych są szyfrowane przy użyciu silnego algorytmu AES-256.
- **Zarządzanie kluczami:** Klucze kryptograficzne są fizycznie i logicznie odseparowane od serwerów aplikacyjnych i przechowywane w dedykowanym, bezpiecznym systemie zarządzania sekretami. Dodatkowo dostawca hostingu zapewnia szyfrowanie na poziomie fizycznych nośników danych.
- **Szyfrowanie danych w ruchu (Encryption in Transit):** Cała komunikacja z Serwisem odbywa się przez bezpieczne, szyfrowane kanały z wykorzystaniem protokołu TLS 1.3, aktywnego mechanizmu HSTS oraz HTTP/3.

3. Autoryzacja i kontrola sesji:

- **Zabezpieczenie sesji:** Autoryzacja użytkowników i procesów w aplikacji realizowana jest w oparciu o bezpieczne, kryptograficznie podpisane tokeny autoryzacyjne.
- **Walidacja danych:** System realizuje ścisłą walidację i filtrowanie wszystkich parametrów wejściowych przesyłanych do aplikacji w celu ochrony przed wstrzykiwaniem złośliwego kodu (np. SQL Injection, XSS).

4. Monitorowanie i dzienniki zdarzeń (Logowanie):

- **Zintegrowany system logów:** Zdarzenia systemowe, błędy aplikacji, próby logowania oraz operacje wykonywane przez użytkowników i administratorów są centralnie rejestrowane i indeksowane za pomocą zaawansowanego stosu analitycznego do analizy logów.
- **Pseudonimizacja logów:** W dziennikach zdarzeń (logach) stosuje się technikę pseudonimizacji – bezpośrednie dane identyfikacyjne użytkowników (takie jak imiona czy nazwiska) są zastępowane wewnętrznymi identyfikatorami systemowymi (ID).

5. Kopie zapasowe i ciągłość działania:

- **Strategia backupów:** Podmiot Przetwarzający realizuje procedurę codziennych, automatycznych kopii zapasowych baz danych.

- **Testy odtworzeniowe:** Integralność i dostępność kopii zapasowych jest regularnie weryfikowana poprzez testowe odtwarzanie danych na odseparowanym środowisku testowym.

6. Testowanie bezpieczeństwa:

- **Weryfikacja podatności:** Poziom bezpieczeństwa infrastruktury oraz podatności aplikacji weryfikowany jest dwuwarstwowo: poprzez zautomatyzowane, cotygodniowe skanowanie kodu i używanych bibliotek (skan zależności OWASP) oraz regularne, kwartalne, zewnętrzne skany podatności infrastruktury sieciowej realizowane za pomocą dedykowanych, uznanych na rynku platform automatyki audytowej.

ZAŁĄCZNIK NR 3
LISTA DALSZYCH PODMIOTÓW PRZETWARZAJĄCYCH

Lp.	Nazwa Dalszego Podmiotu Przetwarzającego	Adres	Miejsce przetwarzania	Cel dalszego powierzenia
1.	DigitalOcean LLC	105 Edgeview Drive, Suite 425, Broomfield, CO 80021, USA	EOG (Centrum danych: Niemcy)	Usługi infrastruktury chmury obliczeniowej
2.	Link Mobility Poland sp. z o.o.	ul. Toszecka 101, 44- 100 Gliwice, Polska	Polska	Usługa automatycznej wysyłki powiadomień SMS

ZAŁĄCZNIK NR 4

CENNIK OBSŁUGI KONTROLI PRZETWARZANIA

Wszystkie koszty zostały podane w kwotach netto (należy doliczyć podatek VAT).

- **130 zł** – Godzina pracy osoby zaangażowanej w Kontrolę Przetwarzania w zakresie audytu środków technicznych, infrastruktury serwerowej oraz kodu.
- **160 zł** – Godzina pracy Inspektora Ochrony Danych (IOD).
- **50 zł** – Godzina pracy pozostałych osób zaangażowanych w Kontrolę Przetwarzania, w szczególności w zakresie audytu dokumentacji prawnej, procedur i rejestrów.