Warszawa, dnia 01.01.2021

OCENA SKUTKÓW DLA OCHRONY DANYCH

WRAZ Z POLITYKĄ BEZPIECZEŃSTWA

1. Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

Dane pozyskiwane będą od klientów za pośrednictwem formularzy interaktywnych na stronach internetowych.

Dane osobowe przetwarzane będą w celach:
- bezpłatnej analizy finansowej, świadczenia usług doradztwa i pośrednictwa finansowego oraz marketingu produktów lub usług przez Administratora oraz przekazania ich bankom, firmom pożyczkowym na podstawie zgody klienta (podstawa prawna – art. 6 ust.1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) zwanego dalej RODO), a okres przetwarzania danych we wskazanym celu wynosił będzie 5 lat od daty ich przekazania
- niezbędnych do wykonania umowy lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (podstawa prawna art. 6 ust.1 lit. b RODO), a okres przetwarzania danych we wskazanym celu wynosił będzie 5 lat od daty ich przekazania
- wypełnienia obowiązku prawnego ciążącego na Administratorze i będą przetwarzane przez okres wymagany przepisami prawa (podstawa prawna art. 6 ust.1 lit. c RODO). Obowiązkiem prawnym nałożonym na Administratora jest w szczególności obowiązek rejestracji i obsługi incydentów bezpieczeństwa informacji – okres przetwarzania danych w tym przypadku wynosi 5 lat od daty incydentu.
- ze względu na prawnie uzasadniony interes realizowany przez Administratora (podstawa prawna - art. 6 ust.1 lit. f RODO), którym jest konieczność przeprowadzania czynności audytowych i kontrolnych (okres przetwarzania 5 lat od daty realizacji czynności), windykacji należności, realizacji zajęć wierzytelności (okres przetwarzania 10 lat od końca roku kalendarzowego, w którym należność powstała)

2. Ocena proporcjonalności operacji przetwarzania do celów przetwarzania.

Operacje przetwarzania są proporcjonalne do celów przetwarzania. Przetwarzanie danych umożliwia łatwy dostęp osób fizycznych do usług finansowych (kredyty, pożyczki) za pośrednictwem Internetu i przyczynia się do budowy społeczeństwa informacyjnego. Zakres pozyskiwanych danych nie wykracza poza cele ich pozyskiwania – dane zasadniczo mają umożliwić Administratorowi oraz bankom i firmom pożyczkowym kontakt z klientem, a także zawarcie i wykonanie umowy.

3. Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

W związku z przekazywaniem danych za pośrednictwem systemów informatycznych istnieje ryzyko, że osoby nieupoważnione spróbują uzyskać do nich dostęp poprzez przełamanie zabezpieczeń. W związku z zastosowaniem środków ochronnych, w tym udostępnianych przez dostawcę hostingu, ryzyko ocenia się na małe.

4. Środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy (polityka bezpieczeństwa).

W celu wyeliminowania ryzyka dostępu do danych osobowych zastosowane zostały następujące środki:
- fizyczny dostęp do nośników danych ograniczony poprzez przechowywanie nośników danych w pomieszczeniach zabezpieczonych przed wstępem osób trzecich
- komputery wykorzystywane w działalności zabezpieczone są hasłem dostępowym oraz posiadają aktualne oprogramowanie antywirusowe wraz z opcją aktualizacji oprogramowania, wyłączona jest opcja autouzupełniania formularzy
- przekazywanie danych odbywa się za pośrednictwem bezpiecznych łączy
- dane przechowywane na zewnętrznych serwerach (cyberfolks.pl) zabezpieczone są przed dostępem osób trzecich przy zastosowaniu środków oferowanych przez dostawę hostingu
- po każdorazowym zakończeniu pracy przy nośnikach danych należy się wylogować
- uzyskanie dostępu do nośników danych następuje na podstawie zgody Administratora poprzez podanie osobie uprawnionej informacji niezbędnych do logowania, z jednoczesnym wyjaśnieniem zasad polityki bezpieczeństwa

W razie stwierdzenia, że doszło do przełamania zabezpieczeń, należy, poza obowiązkami informacyjnymi wynikającymi z RODO, usunąć dane z nośników, do których uzyskała dostęp osoba nieuprawniona, oraz przenieść je na inne nośniki, a także zastosować dodatkowe systemy zabezpieczenia informatycznego.