Umowa powierzenia przetwarzania danych osobowych (DPA)

Niniejsza Umowa powierzenia przetwarzania danych osobowych („Umowa” lub „DPA”) zostaje zawarta w formie dokumentowej (zgodnie z art. 77² Kodeksu cywilnego) z chwilą akceptacji Regulaminu Serwisu i utworzenia Konta w Serwisie Trafjo, pomiędzy:
Klientem (zdefiniowanym w Regulaminie Serwisu), zwanym dalej **„Administratorem”**,
A
Jarosławem Taranek, prowadzącym działalność pod nazwą handlową Trafjo, z adresem do doręczeń: 02-673, Warszawa, Racjonalizacji 3/129, posiadający numer NIP: 5214167585, zwany dalej „Podmiotem przetwarzającym” lub „Procesorem”

§ 1. Definicje

1. **RODO**- Rozporządzenie 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.
2. **Dane osobowe**, **Przetwarzanie**, **Administrator**, **Podmiot przetwarzający**, **Naruszenie ochrony danych osobowych**- pojęcia te mają znaczenie nadane im bezpośrednio w przepisach RODO.
3. **Usługa / Serwis**- usługi walidacji, standaryzacji i poprawy adresów dostaw e-commerce świadczone przez Procesora drogą elektroniczną za pośrednictwem interfejsu API Trafjo oraz platformy webowej Trafjo.

§ 2. Przedmiot umowy i hierarchia dokumentów

1. Administrator powierza Procesorowi przetwarzanie danych osobowych w celu i w zakresie niezbędnym do realizacji Usługi, zgodnie z warunkami określonymi w Regulaminie Serwisu oraz niniejszej Umowie.
2. W przypadku jakichkolwiek sprzeczności pomiędzy postanowieniami Umowy głównej, Regulaminu Serwisu a niniejszą Umową DPA, w zakresie dotyczącym ochrony i przetwarzania danych osobowych bezwzględne pierwszeństwo mają postanowienia niniejszej Umowy.

§ 3. Zakres, kategorie danych i minimalizacja

1. **Kategorie osób, których dane dotyczą:** Klienci końcowi Administratora (sklepu internetowego) składający zamówienia.
2. **Kategorie danych:** Dane obejmują wyłącznie dane lokalizacyjne oraz adresowe

niezbędne do prawidłowej realizacji dostaw e-commerce.

3. **Zakres powierzonych danych (parametry API):** Umowa obejmuje wyłącznie następujące parametry przekazywane za pośrednictwem API lub funkcjonalności Serwisu:
    - systemowe id zamówienia
    - numer zamówienia klienta
    - miasto
    - kod pocztowy
    - ulica (wraz z numerem budynku/lokalu)
    - kraj
4. Procesor nie przetwarza i nie przyjmuje do przetwarzania bezpośrednich danych identyfikacyjnych ani kontaktowych klientów końcowych, takich jak: imiona, nazwiska, adresy e-mail czy numery telefonu.
5. Administrator zobowiązuje się przekazywać wyłącznie dane osobowe minimalne i niezbędne do realizacji celu Usługi. W przypadku, gdy Administrator w ramach pól adresowych (w szczególności w polu ulica) prześle przypadkowo bezpośrednie dane identyfikacyjne lub kontaktowe, Procesor będzie je przetwarzał wyłącznie w zakresie niezbędnym do wykonania usługi walidacji, ich automatycznego odrzucenia lub oczyszczenia. Odpowiedzialność za wprowadzenie tego rodzaju danych do strumienia API spoczywa wyłącznie na Administratorze.
6. Administrator zobowiązuje się przekazywać wyłącznie dane osobowe niezbędne do realizacji celu przetwarzania.

§ 4. Udokumentowane instrukcje i prawo odmowy

1. Administrator instruuje Procesora aby ten przetwarzał dane wyłącznie w zakresie niezbędnym do świadczenia Usług zgodnie z dokumentacją API, konfiguracją integracji, korzystaniem z funkcjonalności Serwisu oraz niniejszą Umową.
2. Procesor przetwarza dane wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Procesor.
3. Procesor natychmiast informuje Administratora, jeżeli jego zdaniem wydane mu polecenie, instrukcja lub konfiguracja stanowi naruszenie RODO lub innych przepisów prawa ochrony danych. Procesor ma prawo odmówić wykonania instrukcji naruszającej przepisy prawa bez ponoszenia odpowiedzialności z tego tytułu.

§ 5. Czas trwania, retencja danych i anonimizacja

1. Dane będą przetwarzane przez Procesora w celach: realizacji walidacji, zapewnienia stabilności systemu, analizy błędów algorytmu oraz obsługi ewentualnych reklamacji.
2. Okres przechowywania (retencji) surowych danych wejściowych w formie logów

systemowych wynosi maksymalnie 90 dni od momentu przesłania zapytania do API. Po tym okresie surowe dane są usuwane lub przekształcane w formę niepozwalającą na identyfikację osoby fizycznej. Dane techniczne i metryki systemowe mogą być przechowywane w formie zagregowanej i nieosobowej, która nie pozwala na identyfikację pojedynczego zapytania ani osoby fizycznej.

3. Strony zgodnie potwierdzają, że dane poddane anonimizacji nie stanowią danych osobowych w rozumieniu RODO i mogą być wykorzystywane przez Procesora do rozwoju, testowania i poprawy algorytmów.
4. Proces anonimizacji ma na celu trwałe uniemożliwienie identyfikacji osoby fizycznej. Obejmuje on w szczególności usunięcie identyfikatorów zamówień (systemowego id zamówienia, numeru zamówienia klienta) oraz transformację, agregację lub skrócenie ciągów adresowych w taki sposób i w takim zakresie, aby w świetle współczesnej wiedzy technicznej oraz przy użyciu racjonalnie dostępnych środków niemożliwe było powiązanie danych z konkretną osobą fizyczną.
5. Administrator może zażądać wcześniejszego usunięcia danych z logów operacyjnych, o ile nie uniemożliwi to realizacji bieżącej usługi lub wykonania obowiązków prawnych Procesora.

§ 6. Obowiązki Procesora, zgłaszanie naruszeń i współpraca

1. Procesor wdroży odpowiednie środki techniczne i organizacyjne określone w Załączniku nr 1 do niniejszej Umowy (zgodnie z art. 32 RODO).
2. Procesor zapewnia, że dostęp do danych posiada wyłącznie ograniczony personel techniczny (programiści i administratorzy) upoważniony do przetwarzania, który zobowiązał się do zachowania tajemnicy.
3. **Współpraca i DPIA:** Procesor, uwzględniając charakter przetwarzania i dostępne informacje, pomaga Administratorowi w realizacji obowiązków odpowiadania na żądania osób, których dane dotyczą, oraz obowiązków wynikających z art. 32–36 RODO (w tym przy przeprowadzaniu ocen skutków dla ochrony danych- DPIA oraz uprzednich konsultacjach z organem nadzorczym).
4. **Zgłaszanie naruszeń:** Procesor zobowiązuje się zgłosić Administratorowi naruszenie ochrony danych osobowych bez zbędnej zwłoki po jego stwierdzeniu, nie później jednak niż w terminie 72 godzin od jego wykrycia. Zgłoszenie przesyłane jest drogą elektroniczną i zawiera:
    - opis charakteru naruszenia oraz przybliżoną liczbę osób/wpisów, których dotyczy,
    - wskazanie kategorii danych,
    - przewidywane skutki oraz sugerowane i wdrożone środki naprawcze.

§ 7. Prawo do audytu

1. Procesor udostępnia Administratorowi informacje niezbędne do wykazania spełnienia

obowiązków z art. 28 RODO oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów (na koszt Administratora, raz w roku kalendarzowym, po 14-dniowym wyprzedzeniu, chyba że wystąpiło naruszenie ochrony danych osobowych lub istnieją uzasadnione przesłanki wskazujące na niezgodność przetwarzania z niniejszą Umową).
2. Audyt nie może prowadzić do ujawnienia tajemnic przedsiębiorstwa Procesora, naruszać bezpieczeństwa innych klientów, ani obejmować dostępu do kodu źródłowego, fizycznej infrastruktury serwerowej czy samodzielnych testów penetracyjnych. Procesor może spełnić swój obowiązek audytowy poprzez udostępnienie odpowiedniej dokumentacji bezpieczeństwa, raportów niezależnych audytorów lub certyfikatów.

§ 8. Podpowierzenie danych (Sub-processing)

1. Administrator wyraża ogólną zgodę na podpowierzenie przetwarzania danych innym podprocesorom w celu utrzymania infrastruktury (kategorie podprocesorów: hosting, utrzymanie serwerów VPS, monitoring i logowanie błędów systemowych). Aktualna lista podprocesorów zawierająca nazwę, funkcję oraz kraj przetwarzania dostępna jest pod adresem: **trafjo.pl/lista-podprocesorow.**
2. Procesor zapewnia, że podprocesorzy są związani obowiązkami ochrony danych nie mniej rygorystycznymi niż określone w niniejszej Umowie.
3. Procesor informuje Administratora o zmianach podprocesorów z 14-dniowym wyprzedzeniem drogą elektroniczną. Administrator ma prawo zgłosić uzasadniony sprzeciw w terminie 14 dni. Brak sprzeciwu oznacza zgodę. W przypadku zgłoszenia sprzeciwu i braku porozumienia, Administrator ma prawo wypowiedzieć DPA ze skutkiem natychmiastowym.
4. Transfer danych poza obszar EOG może odbywać się wyłącznie na podstawie mechanizmów zgodnych z rozdziałem V RODO (np. Standardowe Klauzule Umowne-SCC).

§ 9. Odpowiedzialność i siła wyższa

1. Procesor odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków nałożonych bezpośrednio przez RODO lub działał wbrew zgodnym z prawem instrukcjom Administratora.
2. Łączna odpowiedzialność finansowa Procesora wobec Administratora z tytułu naruszenia niniejszej Umowy w relacjach B2B jest ograniczona do kwoty stanowiącej równowartość opłat wniesionych przez Administratora za Usługi w okresie ostatniego miesiąca poprzedzającego zdarzenie, z wyjątkiem szkód wyrządzonych umyślnie. Ograniczenie to nie narusza bezpośredniej odpowiedzialności wynikającej z art. 82 RODO.
3. Żadna ze Stron nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie obowiązków wynikających z Umowy, jeżeli jest ono następstwem działania siły wyższej

(np. katastrofy naturalne, długotrwałe awarie globalnej sieci szkieletowej, ataki DDoS o skali uniemożliwiającej normalną obronę systemową).

§ 10. Postanowienia końcowe

1. Niniejsza umowa zostaje zawarta na czas trwania umowy głównej. W sprawach nieuregulowanych zastosowanie mają przepisy RODO oraz Kodeksu Cywilnego.
2. Wszelki kontakt oraz zgłoszenia związane z wykonywaniem niniejszej Umowy należy kierować na dedykowany adres e-mail: kontakt@trafjo.pl

---

Załącznik nr 1: Środki Techniczne i Organizacyjne

Procesor oświadcza, że w celu ochrony powierzonych danych osobowych wdrożył i utrzymuje następujące środki bezpieczeństwa:

1. **Lokalizacja i Bezpieczeństwo Infrastruktury:**
    - Wszystkie serwery produkcyjne oraz bazy danych wykorzystywane do świadczenia Usługi są zlokalizowane wyłącznie na terenie Europejskiego Obszaru Gospodarczego (EOG)- m.in. w certyfikowanych centrach danych na terenie Niemiec i Polski (zgodność z normą ISO/IEC 27001).
2. **Bezpieczeństwo Transmisji i Kryptografia:**
    - Wszelka komunikacja z interfejsem API Trafjo oraz platformą webową jest bezwzględnie szyfrowana w tranzycie za pomocą protokołu TLS w wersji minimum 1.2 (z preferencją dla TLS 1.3) przy użyciu silnych algorytmów szyfrujących.
3. **Kontrola Dostępu i Zabezpieczenia Logiczne:**
    - Dostęp do systemów produkcyjnych i baz danych jest rygorystycznie ograniczony (zasada minimalnych uprawnień- RBAC) i przyznawany wyłącznie wybranemu personelowi technicznemu, dla którego dostęp ten jest niezbędny do utrzymania stabilności systemu.
    - Autoryzacja personelu technicznego do infrastruktury chmurowej/VPS wymaga każdorazowo uwierzytelnienia wieloskładnikowego (MFA) oraz bezpiecznych kluczy SSH.
4. **Zarządzanie Podatnościami i Monitoring:**
    - Systemy operacyjne serwerów oraz komponenty oprogramowania (w tym biblioteki Pythona/FastAPI) są regularnie aktualizowane pod kątem poprawek bezpieczeństwa.
    - Procesor prowadzi ciągły monitoring wydajnościowy i bezpieczeństwa (zarządzanie incydentami oraz logowanie prób nieautoryzowanego dostępu).
5. **Kopie Zapasowe:**
    - Procesor regularnie wykonuje kopie zapasowe konfiguracji systemowych oraz baz

danych w celu zapewnienia ciągłości działania i dostępności danych w przypadku awarii. Dostęp do kopii zapasowych jest ograniczony wyłącznie do uprawnionego personelu technicznego