Rejestr czynności przetwarzania

1) Rejestracja konta i utworzenie profilu

1. Nazwa czynności: Rejestracja konta / utworzenie konta Użytkownika w Serwisie
2. Cel(e) przetwarzania:
   a) założenie konta, identyfikacja Użytkownika i osoby kontaktowej, umożliwienie logowania;
   b) weryfikacja podstawowych danych rejestrowych (B2B) i bezpieczeństwo procesu rejestracji;
   c) komunikacja systemowa (np. aktywacja, potwierdzenia, informacje techniczne).
3. Kategorie osób, których dane dotyczą:
   a) osoby kontaktowe / reprezentanci Użytkownika (przedsiębiorcy), tworzący konto;
   b) Użytkownicy (przedsiębiorcy) – dane rejestrowe działalności (nie są danymi osobowymi, ale mogą zawierać elementy osobowe w JDG).
4. Kategorie danych osobowych:
   a) identyfikacyjne i kontaktowe: imię, nazwisko, e-mail (login), (telefon – jeśli podany), stanowisko/funkcja (jeśli podana);
   b) techniczne: IP, identyfikatory sesji, logi rejestracji, data/godzina;
   c) dane firmowe mogą obejmować elementy osobowe w JDG (np. nazwa firmy zawierająca imię i nazwisko).
5. Podstawa prawna:
   a) art. 6 ust. 1 lit. b RODO – podjęcie działań przed zawarciem umowy / zawarcie umowy (konto);
   b) art. 6 ust. 1 lit. f RODO – bezpieczeństwo Serwisu, przeciwdziałanie nadużyciom, weryfikacja poprawności danych w relacji B2B.
6. Kategorie odbiorców danych:
   a) dostawca hostingu/utrzymania, dostawcy IT/oprogramowania, dostawca poczty/transakcyjnych e-maili – jako procesorzy;
   b) podmioty uprawnione (organy) – gdy obowiązek prawny.
7. Przekazywanie do państw trzecich:

co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.

8. Okres przechowywania:
   a) przez czas posiadania aktywnego konta i wykonywania Umowy;
   b) po zakończeniu: w zakresie niezbędnym do roszczeń i bezpieczeństwa zgodnie z polityką retencji; logi rejestracji wg retencji logów.
9. Ogólny opis środków bezpieczeństwa:

TLS/HTTPS, kontrola dostępu, uwierzytelnianie, minimalne uprawnienia, logowanie zdarzeń, backupy, monitoring, procedury incydentowe.

2) Obsługa Umowy i świadczenie usług w Serwisie

1. Nazwa czynności: Realizacja Umowy / świadczenie usług drogą elektroniczną (konto, funkcjonalności, panel)
2. Cel(e):
   a) utrzymanie konta, udostępnienie funkcjonalności zgodnie z pakietem;
   b) zarządzanie uprawnieniami, ustawieniami konta, komunikacja systemowa;
   c) zapewnienie rozliczalności działań w Serwisie (logi operacyjne).
3. Kategorie osób:
   a) osoby kontaktowe/reprezentanci Użytkownika;
   b) użytkownicy korzystający z konta (w tym Użytkownicy Dalsi – w zakresie, w jakim Spółka jest administratorem danych niezbędnych do samego prowadzenia konta i

bezpieczeństwa; dane „wprowadzane" przez Użytkownika mogą podpadać pod rolę procesora po stronie Spółki – odrębna kwalifikacja).

4. Kategorie danych:
   a) dane konta: e-mail/login, imię, nazwisko, ustawienia;
   b) dane dot. korzystania z Serwisu: identyfikatory konta, logi aktywności (data/godzina, operacje), IP, cookies/identyfikatory;
   c) dane komunikacyjne w ramach Serwisu (jeśli istnieją funkcje wiadomości).
5. Podstawa prawna:
   a) art. 6 ust. 1 lit. b RODO – wykonanie Umowy;
   b) art. 6 ust. 1 lit. f RODO – bezpieczeństwo, rozliczalność, przeciwdziałanie nadużyciom.
6. Odbiorcy:
   a) dostawcy IT/hostingu, narzędzi wspierających działanie Serwisu (procesorzy);
   b) podmioty uprawnione prawem.
7. Transfery: co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.
8. Retencja:
   a) przez czas obowiązywania Umowy;
   b) po zakończeniu: dane rozliczeniowe/księgowe wg prawa; logi i dane techniczne wg retencji bezpieczeństwa; pozostałe dane – usunięcie/anonimizacja wg polityki retencji.
9. Zabezpieczenia: segmentacja uprawnień kont, TLS/HTTPS, kontrola dostępu, uwierzytelnianie, minimalne uprawnienia, logowanie zdarzeń, backupy, monitoring, procedury incydentowe

3) Fakturowanie i rozliczenia

1. Nazwa czynności: Fakturowanie / rozliczenia / księgowość
2. Cel(e):
   a) wystawianie i przesyłanie faktur, rozliczenia płatności, ewidencja księgowa;
   b) spełnienie obowiązków podatkowych i rachunkowych.
3. Kategorie osób:
   a) osoby kontaktowe/odbiorcy faktur po stronie Użytkownika;
   b) jednoosobowe działalności – dane osobowe przedsiębiorcy w danych firmowych.
4. Kategorie danych:
   a) dane do faktury: nazwa/firmowe, NIP, adres, ewentualnie imię/nazwisko w JDG;
   b) e-mail do wysyłki faktur;
   c) dane płatnicze/rozliczeniowe (np. rachunek, identyfikator transakcji, historia płatności).
5. Podstawa prawna:
   a) art. 6 ust. 1 lit. c RODO – obowiązek prawny (podatki/rachunkowo
   b) art. 6 ust. 1 lit. b RODO – wykonanie Umowy (rozliczenie usługi).
6. Odbiorcy:
   a) biuro rachunkowe / system księgowy (procesor lub odrębny administrator – zależnie od relacji i dostępu);
   b) operator płatności/bank (odrębny administrator w zakresie transakcji);
   c) dostawcy IT (procesorzy).
7. Transfery: co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.
8. Retencja:
   a) dokumenty księgowe zgodnie z przepisami podatkowymi/rachunkowymi (co do zasady min. 5 lat, liczonych wg właściwych przepisów);
   b) pozostałe dane rozliczeniowe – do przedawnienia roszczeń i wymogów prawnych.

9. Zabezpieczenia: kontrola dostępu, szyfrowanie transmisji, ograniczenie osób z dostępem do danych finansowych.

4) Wsparcie, kontakt i reklamacje

1. Nazwa czynności: Obsługa zgłoszeń, reklamacji, zapytań (e-mail/formularz/helpdesk)
2. Cel(e):
    a) udzielanie odpowiedzi, obsługa reklamacji, wsparcie techniczne;
    b) dokumentowanie przebiegu zgłoszeń (dowodowo i jakościowo).
3. Kategorie osób:

osoby kontaktujące się (Użytkownicy / osoby działające w imieniu Użytkownika).

4. Kategorie danych:
    a) imię/nazwisko (jeśli podane), e-mail, telefon (jeśli podany);
    b) treść korespondencji i załączniki;
    c) metadane zgłoszenia (daty, identyfikator konta, status).
5. Podstawa prawna:
    a) art. 6 ust. 1 lit. b RODO – realizacja Umowy (support);
    b) art. 6 ust. 1 lit. f RODO – obrona przed roszczeniami, zapewnienie jakości, dowodowość
6. Odbiorcy:
    a) dostawca helpdesku (jeśli używany) – procesor;
    b) kancelaria prawna – odrębny administrator lub procesor (zależnie od zlecenia);
    c) podmioty uprawnione prawem.
7. Transfery: co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.
8. Retencja:

co najmniej przez czas obsługi zgłoszenia + okres niezbędny dla roszczeń (wg polityki retencji, typowo do przedawnienia roszczeń związanych z Umową).

9. Zabezpieczenia: ograniczenie dostępu do ticketów, kontrola uprawnień, szyfrowanie transmisji.

5) Logi bezpieczeństwa i przeciwdziałanie nadużyciom

1. Nazwa czynności: Logowanie zdarzeń, monitoring bezpieczeństwa, antyfraud
2. Cel(e):
    a) zapewnienie bezpieczeństwa Serwisu, wykrywanie incydentów, analiza nadużyć;
    b) utrzymanie ciągłości działania i integralności usług;
    c) dowodowość na potrzeby incydentów i roszczeń.
3. Kategorie osób:

użytkownicy kont, osoby logujące się, osoby odwiedzające (w zakresie danych technicznych).

4. Kategorie danych:

IP, identyfikatory sesji, user-agent, identyfikator konta, daty/godziny, logi logowań/operacji, alerty systemowe.

5. Podstawa prawna:

art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes (bezpieczeństwo, nadużycia, roszczenia).

6. Odbiorcy:
    a) dostawcy IT;
    b) organy uprawnione (w razie incydentów / obowiązków).
7. Transfery: co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.
8. Retencja:

zgodnie z polityką retencji.

9. Zabezpieczenia: segmentacja, dostęp tylko dla upoważnionych, integralność logów, backup, monitoring.

6) Marketing

1. Nazwa czynności: Marketing bezpośredni usług i funkcjonalności Serwisu StrefaRP.org
2. Cel(e):
   a) wysyłka informacji marketingowych drogą e-mail;
   b) kontakt telefoniczny/SMS w celach marketingowych (jeśli zgoda).
3. Kategorie osób:
osoby kontaktowe Użytkownika, które wyraziły zgodę marketingową.
4. Kategorie danych:
e-mail, telefon (jeśli zgoda telefoniczna), identyfikator konta, historia zgód, logi wysyłek.
5. Podstawa prawna:
art. 6 ust. 1 lit. a RODO – zgoda;
dodatkowo: zgody kanałowe wymagane przepisami szczególnymi (e-mail/telefon) – do wdrożenia w mechanice checkboxów i logowaniu.
6. Odbiorcy:
narzędzie do mailingów/SMS (procesor);
dostawcy IT.
7. Transfery: co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.zależnie od narzędzi (SCC/TIA).
8. Retencja:
do czasu wycofania zgody + okres niezbędny do wykazania rozliczalności (dowód zgody) zgodnie z polityką retencji.
9. Zabezpieczenia: rejestr zgód (treść, data, kanał, identyfikator), możliwość łatwego wycofania.

7) Windykacja i dochodzenie/obrona roszczeń

1. Nazwa czynności: Windykacja należności, dochodzenie/obrona roszczeń
2. Cel(e):
   a) odzyskanie należności, prowadzenie korespondencji przedsądowej;
   b) obrona przed roszczeniami i zabezpieczenie dowodów.
3. Kategorie osób:
osoby kontaktowe/reprezentanci Użytkownika (w tym JDG).
4. Kategorie danych:
dane identyfikacyjne i kontaktowe, dane fakturowe/rozliczeniowe, historia płatności, korespondencja.
5. Podstawa prawna:
   a) art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes (dochodzenie/obrona roszczeń);
   b) art. 6 ust. 1 lit. c RODO – jeżeli wynika z obowiązków prawnych przechowywania dokumentów.
6. Odbiorcy:
   a) kancelaria prawna, firma windykacyjna (odrębny administrator lub procesor – do kwalifikacji i umów);
   b) sądy/komornik/instytucje uprawnione.
7. Transfery: co do zasady brak; jeżeli używane narzędzia dostawców spoza EOG – transfer na podstawie SCC i oceny transferu (TIA), zgodnie z Polityką Prywatności.
8. Retencja:
do czasu zakończenia sprawy + okres przedawnienia/archiwizacji zgodnie z polityką retencji.

9. Zabezpieczenia: ograniczenie dostępu, kontrola uprawnień, bezpieczna wymiana dokumentów.