Polityka Ochrony Danych Osobowych (RODO)

United Heritage Finance Sp. z o.o.

1. Cele polityki:

- Zapewnienie zgodności z **Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)**.
- Ochrona danych osobowych klientów, partnerów, kontrahentów i pracowników.
- Minimalizacja ryzyka naruszeń bezpieczeństwa danych i sankcji prawnych.

2. Zakres stosowania:

- Wszystkie dane osobowe przetwarzane przez spółkę w Polsce i w relacjach międzynarodowych (Ukraina, EU, USA i inne).
- Dane klientów, partnerów biznesowych, pracowników i kandydatów.
- Dane przetwarzane w systemach IT, dokumentach papierowych i komunikacji elektronicznej.

3. Podstawy prawne przetwarzania danych:

- RODO – art. 6 i 9 (zgoda, umowa, obowiązek prawny, prawnie uzasadniony interes).
- Kodeks pracy i przepisy sektorowe (doradztwo, finanse, AML/KYC).
- Przepisy sankcyjne UE, Polski, USA – weryfikacja kontrahentów.

4. Zasady przetwarzania danych:

- **Legalność, rzetelność i przejrzystość**
- **Minimalizacja danych** – tylko niezbędne informacje.
- **Ograniczenie celu** – dane wykorzystywane wyłącznie w określonym celu.
- **Dokładność** – bieżąca aktualizacja danych.
- **Bezpieczeństwo** – odpowiednie środki techniczne i organizacyjne (szyfrowanie, dostęp ograniczony).
- **Ograniczenie przechowywania** – dane przechowywane zgodnie z przepisami i polityką archiwizacji.

5. Prawa osób, których dane dotyczą:

- Prawo dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu.
- Prawo wniesienia skargi do PUODO (Polski Urząd Ochrony Danych Osobowych) i odpowiednich organów międzynarodowych.

6. Obowiązki pracowników:

- Zachowanie poufności danych.
- Zgłaszanie incydentów naruszenia danych do IOD.
- Udział w szkoleniach i stosowanie procedur bezpieczeństwa.

7. Przekazywanie danych do podmiotów zewnętrznych:

- Dane mogą być przekazywane podmiotom przetwarzającym (procesorom) na podstawie umowy powierzenia danych.
- Weryfikacja zgodności podmiotów z RODO i standardami bezpieczeństwa.

8. Incydenty i naruszenia danych:

- Każdy incydent bezpieczeństwa należy zgłosić do IOD w ciągu 24 godzin.
- IOD prowadzi rejestr naruszeń i podejmuje działania korygujące.

9. Szkolenia i świadomość:

- Obowiązkowe szkolenia dla wszystkich pracowników i członków Zarządu.
- Regularne przypomnienia i aktualizacje w intranecie.

10. Audyt i monitoring:

- Coroczny audyt RODO przeprowadzany przez IOD lub podmiot zewnętrzny.
- Raportowanie Zarządowi o stanie ochrony danych.

11. Procedury operacyjne i instrukcje wewnętrzne

1. **Instrukcja powierzenia danych osobowych podmiotom zewnętrznym**
2. **Procedura obsługi żądań osób, których dane dotyczą**
3. **Procedura zgłaszania naruszeń danych osobowych**
4. **Rejestr kategorii danych przetwarzanych w spółce**
5. **Procedura archiwizacji i usuwania danych**
6. **Instrukcja bezpieczeństwa IT i komunikacji elektronicznej**

12. Wzorce dokumentów dla pracowników i klientów

1. **Formularz zgody na przetwarzanie danych osobowych** (klienci, partnerzy)
2. **Deklaracja poufności dla pracowników**
3. **Formularz zgłoszenia incydentu RODO**
4. **Checklista due diligence RODO dla partnerów i kontrahentów**

Data przyjęcia przez Zarząd: 1 grudnia 2025 r.