[NAZWA FIRMY]

Procedura weryfikacji podmiotu przetwarzającego

Wersja	
Właściciel	
Data zatwierdzenia	
Data wejścia w życie	
Zatwierdzający	

SPIS TREŚCI

§ 1. DEFINICJE

1. **Administrator (ADO) / [NAZWA FIRMY]** – spółka ..... z siedzibą .....

2. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

3. **Inspektor Ochrony Danych Osobowych (IOD) / Koordynator ds. RODO** – osoba, wyznaczona przez Administratora do pełnienia funkcji inspektora ochrony danych osobowych zgodnie z RODO / koordynatora ochrony danych;

4. **Pracownik** – osoba świadcząca pracę u Administratora - bez względu na formę zatrudnienia;

5. **Procedura** – niniejszy dokument;

6. **Przetwarzanie danych osobowych** – oznacza jakąkolwiek operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7. **Podmiot przetwarzający (PP)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza lub będzie przetwarzał dane osobowe w imieniu Administratora;

8. **RODO** – Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych osobowych);

9. **Umowa powierzenia przetwarzania** – podstawa prawna powierzenia przetwarzania danych osobowych na zlecenie Administratora, zawarta zgodnie z wymaganiami wskazywani w art. 28 RODO.

§ 2. CEL I ZAKRES PROCEDURY

1. Celem niniejszej Procedury jest zapewnienie bezpieczeństwa przetwarzania danych osobowych zarówno przez Administratora, jak i Podmiot przetwarzający, któremu spółka zamierza powierzyć przetwarzanie danych osobowych poprzez odpowiednią weryfikację takiego podmiotu.

2. Procedura została opracowana w oparciu o szczególne wymogi jakie przepisy o ochronie danych osobowych nakładają na Administratora.

3. Procedura obowiązuje od dnia zatwierdzenia jej przez zarząd Administratora. Zmiany i przegląd Procedury dokonywane są przez Koordynatora ds. RODO.

§ 3. POSTĘPOWANIE Z PODMIOTEM PRZETWARZAJĄCYM

1. W przypadku powierzenia przetwarzania danych osobowych w imieniu i na rzecz Administratora, przed zawarciem umowy powierzenia przekazuje się Podmiotowi przetwarzającemu arkusz weryfikacyjny o którym mowa w § 4, stanowiący Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych (dalej: „**Arkusz**").

2. Podmiot przetwarzający jest zobowiązany uzupełnić Arkusz oraz odesłać go podpisany we wskazanym terminie do Pracownika koordynującego proces zawarcia Umowy powierzenia przetwarzania.

3. Administrator lub Pracownik koordynujący proces zawierania Umowy powierzenia przetwarzania przekazuje uzupełniony Koordynatorowi ds. RODO w celu dokonania oceny oświadczeń Podmiotu przetwarzającego zawartych w Arkuszu. Ocena jest dokonywana poprzez umieszczenie adnotacji na Arkuszu stwierdzającej czy Podmiot przetwarzający spełnia wymogi RODO w zakresie przetwarzania danych. W braku takiej adnotacji przyjmuje się, że Podmiot przetwarzający spełnia wymogi i został dopuszczony do współpracy.

4. Administrator pouczył Pracowników, że sytuacja w której w toku wykonywania np. umowy o świadczenie usług informatycznych przekazywane są Administratorowi dane osobowe pracowników innych podmiotów (klientów), to wówczas nie zachodzi relacja powierzenia danych osobowych i niniejsza Procedura nie ma zastosowania.

5. Koordynator ds. RODO archiwizuje uzupełniony Arkusz. Arkusz przechowywany jest rok po zakończeniu współpracy z Podmiotem przetwarzającym.

§ 4. AUDYT

Na podstawie przepisów RODO (oraz zawartych umów powierzenia), Administrator ma prawo okresowo weryfikować Podmiot przetwarzający pod kątem spełnienia wymogów RODO. O sposobie i częstotliwości kontroli decyduje Administrator w miarę uzasadnionych potrzeb i zasobów własnych.

Załącznik nr 1. Arkusz weryfikacyjny podmiotu przetwarzającego

ARKUSZ WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE

Podmiot przetwarzający:
Dane kontaktowe podmiotu przetwarzającego:

ARKUSZ WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE				
	Lp.	**Treść pytania**	**Odpowiedź podmiotu przetwarzającego dane osobowe**	**Uwagi/ Komentarze**
	Kwestie organizacyjne			
	1.	Czy podmiot przetwarzający dane osobowe (**„PPDO"**) wyznaczył Inspektora Ochrony Danych?	Tak / Nie	
	2.	Jeżeli nie został wyznaczony IOD, to prosimy o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu: _____	
	3.	Czy PPDO wprowadził środki techniczne i organizacyjne, które będą spełniały wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych oraz będą chroniły prawa osób, których dane dotyczą?	Tak / Nie	
	4.	Czy PPDO korzysta z dalszych procesorów w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych?	Tak / Nie	
	5.	Jeżeli PPDO korzysta z dalszych procesorów to czy są oni zlokalizowani w ramach EOG?	Tak / Nie	
	6.	Czy dalsi procesorzy stosują środki techniczne i organizacyjne spełniające wymogi RODO?	Tak / Nie	
	7.	Jeżeli transfer danych odbywa		

		się poza EOG to na jakiej podstawie prawnej?		
	Kwestie proceduralne			
	1.	Czy PPDO prowadzi rejestr czynności dla powierzonych operacji przetwarzania danych osobowych?	Tak / Nie	
	2.	Czy PPDO wdrożył procedury dotyczące zarzadzania incydentami bezpieczeństwa?	Tak / Nie	
	Kwestie bezpieczeństwa			
	1.	Czy PPDO wprowadził środki zapewniające, że systemy IT używane do przetwarzania danych osobowych są zgodne z RODO oraz innymi aktami regulującymi przetwarzanie danych osobowych?	Tak / Nie	
	2.	Czy PPDO przechodzi regularne audyty z zakresu bezpieczeństwa danych? Jeśli tak to czy może udostępnić raporty?	Tak / Nie	
	3.	Czy PPDO posiada aktualny certyfikat ISO 27001 lub inne równoważny np. PCI?	Tak / Nie	

Oświadczenie:
W imieniu Podmiotu przetwarzającego dane osobowe oświadczam, że powyżej przekazane informacje są zgodne z prawdą. W przypadku zmiany któregokolwiek z ww. elementów, zobowiązuje się niezwłocznie (nie później niż w terminie 7 dni od wystąpienia zdarzenia) powiadomić o tym administratora danych osobowych.

_____ data

_____ podpis