**Polityka Ochrony Danych Osobowych**

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” („**Polityka**”) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w działalności gospodarczej prowadzonej pod firmą Anna Lewandowska („**Podmiot**”).
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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) („**RODO**”) i stanowi podstawowy dokument regulujący zasady przetwarzania danych osobowych w Podmiocie z wymogami RODO.
3. Za wdrożenie i utrzymanie niniejszej Polityki odpowiada Anna Lewandowska. Do stosowania zasad niniejszej Polityki oraz wszelkich innych regulacji związanych z ochroną danych osobowych, w szczególności przepisów RODO oraz krajowej ustawy o ochronie danych osobowych zobowiązani są wszyscy pracownicy oraz współpracownicy Podmiotu.
4. **Skróty i definicje:**

**Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

**RODO** oznaczarozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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).

**Dane** oznaczają dane osobowe w rozumieniu RODO.

**Dane wrażliwe** oznaczają dane szczególnej kategorii określone w art. 9 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej i dane karne, tj. dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

**Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

**Podmiot przetwarzający** oznacza organizację lub osobę, której Podmiot powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).

**Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

**Transfer danych** oznacza przekazanie danych do państwa trzeciego (poza Europejski Obszar Gospodarczy) lub organizacji międzynarodowej.

**RCPD** oznacza Rejestr Czynności Przetwarzania Danych Osobowych

**Rejestr** oznacza RCPD lub Rejestr Kategorii Czynności Przetwarzania Danych Osobowych podmiotu przetwarzającego.

**Podmiot** oznacza indywidualną działalność gospodarczą Anny Lewandowskiej prowadzącą działalność gospodarczą pod firmą Anna Lewandowska, adres; ul. Książenicka 76D, 05-807 Podkowa Leśna

* 1. Podmiot dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
  2. Podmiot zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
  3. Podmiot umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
  4. Podmiot na bieżąco dokumentuje to, w jaki sposób spełnia obowiązki wynikające z RODO, aby w każdej chwili móc wykazać zgodność.

1. **Zasady przetwarzania Danych**

Podmiot przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2. rzetelnie i uczciwie (rzetelność);
3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4. w konkretnych celach i nie „na zapas” (minimalizacja);
5. nie więcej niż potrzeba (adekwatność);
6. z dbałością o prawidłowość danych (prawidłowość);
7. nie dłużej niż potrzeba (czasowość);
8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
9. **Inwentaryzacja danych.** Podmiot stale dokonuje identyfikacji zasobów przetwarzanych danych osobowych, w tym:
10. przypadków przetwarzania danych wrażliwych - w przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Podmiot przetwarza je zgodnie z RODO;
11. przypadków przetwarzania danych osób, których nie identyfikuje („**dane niezidentyfikowane**”);
12. przypadków przetwarzania danych dzieci;
13. profilowania;
14. współadministrowania danymi.
15. **Rejestr.** Podmiot prowadzi i utrzymuje Rejestr. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Podmiocie.
    1. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności. Rejestr jest prowadzony w formie elektronicznej, w formacie pliku excel.
    2. W Rejestrze, dla każdej czynności przetwarzania danych, którą Podmiot uznał za odrębną dla potrzeb Rejestru, Podmiot odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Podmiotu, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.
    3. W celu zapewnienia aktualności Rejestru podlega on aktualizacji przy każdej nowej czynności przetwarzania danych, nie rzadziej jednak niż raz na miesiąc.
    4. W przypadku kontroli organu nadzorczego Rejestr jest udostępniany na żądanie Urzędu Ochrony Danych Osobowych niezwłocznie.
    5. Wzór Rejestru stanowi ***Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”*.** Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Podmiot rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.
16. **Podstawy prawne.** Podmiot zapewnia, identyfikuje i weryfikuje podstawy prawne przetwarzania Danych i rejestruje je w Rejestrze. W przypadku, gdy podstawą przetwarzania Danych jest uzasadniony interes administratora danych, Podmiot uszczegóławia uzasadnienie takich przypadków.
17. **Obsługa praw jednostki.** Podmiotspełnia obowiązki informacyjne względem osób, których dane dotyczą.
    1. **Sposób obsługi praw jednostki i obowiązków informacyjnych**
       1. Podmiot dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
       2. Podmiot dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
       3. Podmiot wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
       4. W celu realizacji praw jednostki Podmiot zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Podmiot, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
       5. Podmiot dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób wykonywanych w Podmiocie.
    2. **Obowiązki informacyjne**
       1. Podmiot wykonuje obowiązki informacyjne wobec osób, których dane dotyczą przejrzyście i czytelnie, zgodnie z zakresem przewidzianym w art. 13 i 14 RODO.
       2. Podmiot informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
       3. Podmiot informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej maksymalnie w terminie miesiąca od pozyskania danych.
       4. Podmiot informuje o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym)
       5. Podmiot informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
       6. Podmiot informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
       7. Podmiot bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
    3. **Realizacja praw osób, których dane dotyczą**
       1. Żądania osób, których dane dotyczą związane z realizacją ich praw realizowane są przez Podmiot.
       2. **Odmowa**. Podmiot informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
       3. **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, Podmiot informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych) a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem że kopii danych wydanej w wykonaniu prawa dostępu do danych Podmiot nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
       4. **Kopie danych**. Na żądanie Podmiotu wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania kopii danych.
       5. **Sprostowanie danych**. Podmiot dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Podmiot ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby
       6. **Uzupełnienie danych**. Podmiot uzupełnia i aktualizuje dane na żądanie osoby. Podmiot ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Podmiot nie musi przetwarzać danych, które są Podmiotowi zbędne). Podmiot może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Podmiot procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
       7. **Usunięcie danych**. Na żądanie osoby, Podmiot usuwa dane, gdy
       8. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach
       9. zgoda na ich przetwarzanie została cofnięta a nie ma innej podstawy prawnej przetwarzania
       10. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych
       11. dane były przetwarzane niezgodnie z prawem
       12. konieczność usunięcia wynika z obowiązku prawnego
       13. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej)

Podmiot zapewnia sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki o których mowa w art. 17. ust. 3 RODO.

* + 1. **Ograniczenie przetwarzania. Podmiot dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:**

1. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość
2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania
3. Podmiot nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń
4. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Podmiotu zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu

W trakcie ograniczenia przetwarzania Podmiot przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego .

Podmiot informuje osobę przed uchyleniem ograniczenia przetwarzania.

* + 1. **Przenoszenie danych.** Na żądanie osoby Podmiot wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Podmiotowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Podmiotu.
    2. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Podmiot w oparciu o uzasadniony interes Podmiotu, Podmiot uwzględni sprzeciw o ile nie zachodzą ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
    3. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Podmiot uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

1. **Minimalizacja.** Podmiot posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
2. zasady zarządzania adekwatnością danych – Podmiot weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania; dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok; przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).
3. zasady reglamentacji i zarządzania dostępem do danych – Podmiot stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe); dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających; dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
4. zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności – Podmiot kontroluje cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
5. **Bezpieczeństwo.** Podmiot zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
6. przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
7. przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
8. dostosowuje środków ochrony danych do ustalonego ryzyka;
9. posiada system zarządzania bezpieczeństwem informacji;
10. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.
11. **Przetwarzający.** Podmiot posiada zasady doboru przetwarzających dane na rzecz Podmiotu, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia zgodne z art. 28 RODO. Podmiot przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące ***Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”***.
12. **Transfer danych.** Podmiot nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce.
13. **Przetwarzanie transgraniczne.** Nie występują w przypadku Podmiotu.

**Załączniki:**

1. ***Wzór Rejestru Czynności Przetwarzania Danych***
2. ***Wzór umowy powierzenia przetwarzania danych***