POLITYKA OCHRONY DANYCH OSOBOWYCH
(Polityka Prywatności)

I. INFORMACJE OGÓLNE

1. Mając na uwadze należyte postępowanie z zakresu ochrony i przetwarzania danych osobowych, pragniemy zauważyć, iż niniejszy dokument zatytułowany "Polityka Ochrony Danych Osobowych" ma za zadanie stanowić przewodnik po zasadach i regulacjach z zakresu przetwarzania danych osobowych w Naszej działalności czyli u Przedsiębiorcy pod firmą FIOLETOW.PL SARA SWOBODA z siedzibą Witnica ul. Komisji Edukacji Narodowej 3, 66-460 Witnica adres do korespondencji: Mikołaja Kopernika 10, 66-470 Kostrzyn nad Odrą tel: 695 555 727 email: kontakt@fioletow.pl lub prawny@fioletowo.pl.
2. Ochrona danych osobowych jest ważnym aspektem polityki naszej działalności. Jako podmiot świadczący usługi na rzecz osób fizycznych oraz osób prawnych, mamy poczucie odpowidzialniości za dane osobowe przetwarzane przez nas w związku z prowadzoną działalnością gospodarczą.
3. Polityka ochrony danych osobowych zawiera opis podstawowych zasad ochrony danych osobowych obowiązujących u Administratora, poltyka ochrony danych osobowych zwiera również odwołania do załaczników w tym min. klauzuli Informacyjnej o Przetwarzaniu Danych Osobowych dla klientów i współpracowników oraz klauzuli Informacyjnej dla pracowników.
4. Za wdrożenie i utrzymanie, przestrzeganie zmian w przepisach prawa, auktualizację dokumentacji niniejszej Polityki odpowiedzialny jest adminstrator.
5. Adminstrator powinien zapewnić zgodność postępowania kontrahentów administratora z niniejszym dokumentem w odpowiednim zakresie gdy dochodzi do przekazania im danych osobowych przez adminstratora.
6. Zapisy zawarte w Naszych dokumentach wyczerpują obowiązki informacyjne zawarte w art. 13 RODO, które to zapisy administrator starał się przedstawić w sposób przejrzysty, zwięzły, zrozumiały w jak najbardziej uproszczonej formie.
7. W przypadku jakichkolwiek wątpliwości osoba której dane dotyczą może zwrócić się o dalsze wyjaśnienia zgodnie z adresami kontakowymi przedstawionymi w niniejszym dokumencie.

II. ZAKRES POJĘĆ, DEFINICJE, SKRÓTY

1. **POLITYKA** oznacza ninejszą Politykę Ochrony Danych Osobowych, o ile co innego nie wynika z kontekstu.
2. **RODO** oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016r. w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporzadzenie o ochronie danych) [Dz.UZ. UE I.119, s.1].
3. **USTAWA O OCHRONIE DANYCH OSOBOWYCH** oznacza ustawę z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późniejszymi zmianami).
4. **USTAWA O ŚWIADCZENIU USŁUG DROGĄ ELEKTRONICZNĄ** oznacza ustawę z dnia 18 lipca 2002r. (Dz.U. 2017 poz. 1219).
5. **USTAWA PRAWO TELEKOMUNIKACYJNE** oznacza ustawę z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz.U. 2017 poz. 1907 z późniejszymi zmianami).
6. **IOD** oznacza Inspektor Ochrony Danych Osobowych.
7. **ADMINSTRATOR** oznacza Przedsiębiorcy pod firmą FIOLETOW.PL SARA SWOBODA z siedzibą Witnica ul. Komisji Edukacji Narodowej 3, 66-460 Witnica adres do korespondencji: Mikołaja Kopernika 10, 66-470 Kostrzyn nad Odrą tel: 695 555 727 email: kontakt@fioletow.pl lub prawny@fioletowo.pl.
8. **PRACODAWCA** oznacza Przedsiębiorcy pod firmą FIOLETOW.PL SARA SWOBODA z siedzibą Witnica ul. Komisji Edukacji Narodowej 3, 66-460 Witnica adres do korespondencji: Mikołaja Kopernika 10, 66-470 Kostrzyn nad Odrą tel: 695 555 727 email: kontakt@fioletow.pl lub prawny@fioletowo.pl.
9. **PRACOWNIK** oznacza osoby pozostające z pracodawcą w stosunku pracy.
10. **UODO** oznacza Urząd Ochrony Danych Osobowych.
11. **DANE** oznacza dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
12. **REJESTR** oznacza Rejstr Czynności Przetwarzania Danych Osobowych.
13. **EKSPORT DANYCH** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
14. **DANE SZCZEGÓLNYCH KATEGORI** oznacza dane wymienione w art. 9 ust. 1 RODO czyli m.in. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależnośc do związków zawodowych.

15. **DANE KARNE** oznaczają dane wymienone w art. 10 RODO czyli dane dotyczące wyroków skazujących i naruszeń prawa.
16. **DANE DZIECI** oznaczają dane osób poniżej 16 roku życia

III. ZASADY OCHRONY DANYCH OSOBOWYCH

1. POSTANOWIENIA OGÓLNE

1. Administrator dba o ochronę prywatności i przetwarza dane osobowe zgodnie z prawem, zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie zmierzające do pogłębienia wiedzy, dostosowania przepisów oraz udoskonalenia zasad bezpieczeństwa.
2. Administrator umożliwia osobom, których dane przetwarza wykonywanie swoich praw i obowiązków i te prawa realizuje.
3. Ochrona Danych Osobowych u administratora opiera się na czterch podstawowych filarach:
   a) **Legalność –** administrator dba ochronę prywatności i przetwarzania danych osobowych zgodnie z prawem, starając się aktualizować dokumentację stosownie do zmieniających się przepisów prawa;
   b) **Bezpieczeństwo –** administrator stara się zapewnić odpowiedni stopień bezpieczeństwa danych osobowych, które przechowuje lub przetwarza, ciągle podejmując działania w tym zakresie poprzez udoskonalanie zabezpieczeń i procedur z tym związanych;
   c) **Prawa jednostki –** administrator umozliwia osobom, których dane przechowuje lub przetwarza wykonywanie swoich praw;
   d) **Rozliczalność –** administrator dokumentuje w jaki sposób spełnia obowiązki nałożone przez RODO aby w każdej chwili móc wykazać zgodność z założeniami RODO.
4. Administrator przetwarza dane osobowe z poszanowaniem nastepujących zasad:
   a) w sposób rzetelny i utrzciwy;
   b) w sposób przejrzysty dla osoby, której dane dotyczą;
   c) w konkretnych celach i nigdy na zapas;
   d) ze szczególną dbałością o zgodność danych z rzeczywistością;
   e) nie dłużej niż potrzeba:
   f) zapewniając odpowiednie bezpieczeństwo danych.

2. SPOSOBY ZABEZPIECZANIA DANYCH

1. Administrator zapewnia poziom bezpieczeństwa danych osobowych poprzez ograniczony dostęp do danych osobowych przez kontrolę dostępu fizycznego w tym m.in:
   a) zabezpieczenie danych w odpowiedni sposób w zamknięciu, aby nie mogły się dostać do nich osoby niepożądane;
   b) zamykanie pomieszczeń, zamykanie kasetek, sejfów oraz innego rodzaju szaf i biurek z zawartością danych osobowych;
   c) nie umieszczenie dokumentów lub urządzeń z danymi osobowymi w widocznym miejscu, łatwo dostępnym dla osób postronych, umieszczanie kluczy do pomieszczeń w zabezpieczonych gablotach lub pod kontrolą wyspecjalizowanych organów lub powołanych do tego osób;
   d) komputer, tablet, laptop, telefon lub inne tegoż rodzaju urządzenia na których znajdują się dane osobowe użytkowany jest tylko przez administratora i osoby przez niego upoważnione;
   e) komputer, tablet, laptop, telefon, w którym znajdują się dane osobowe wyposażono w indywidualną ochronę antywirusową;
   f) hasło zabezpieczające komputer, laptop, telefon, tablet na którym znajdują się dane osobowe jest zindywidualizowane przez administratora i znane tylko administratorowi;
2. Administrator zapewnia poziom bezpieczeństwa danych osobowych poprzez prawne ograniczenie dostępu w tym m.in:
   a) zobowiązania administratora do zachowania poufności przez współpracowników, klientów, kontrahentów;
   b) informowanie o sposobie ochrony danych stosowanego przez administratora współpracowników, klientów, kontrahentów współpracujących z administratorem;
3. Administrator zapewnia poziom bezpieczeństwa także poprzez:
   a) logiczne zabezpieczenie (ograniczenie uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych w których rezydują dane osobowe);
   b) dostosowanie środków ochrony do ustalonego ryzyka;
   c) stosowanie procedury pozwalającej na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia

ochrony danych Urzędowi Ochrony Danych – zarządza incydentami;

3. PRAKTYKI STOSOWANE PRZEZ ADMINISTRATORA W CELU OCHRONY DANYCH OSOBOWYCH

1. Administrator dokonuje wyrzucenia dokumentów zawierających dane osobowe dopiero po uprzednim ich trwałym zniszczeniu za pomocą urządzeń do tego służących lub w tradycyjny sposób mechaniczny;
2. Administrator nie pozostawia dokumentów w miejscach ogólnodostepnych w trakcie pracy oraz po zakończeniu pracy;
3. Administrator nie pozostawia dokumentów czy kopii dokumentów w miejscu widocznym, drukarkach, kserokopiarkach, skanerach czy innych podobnych urzadzeniach;
4. Administrator nie pozostawia osób trzecich bez nadzoru w pomieszczeniach, w których znajdują się dokumenty zawierające dane osobowe;
5. Administrator zwraca szczególną uwagę, żeby nie pozostawiać kluczy w drzwiach, szafkach, biurkach, w których znajdują się dane osobowe;
6. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają znszczeniu neutralizuje się za pomocą urzadzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na oddtworzenie ich treści;
7. Dokumenty i nośniki informacji zawierające dane osobowe po zakończeniu pracy przechowywane są w zamykanych na klucz szafkach.
8. Administrator dba o czytelność i styl przkazywanych informacji oraz o czytelną komunikację z osobami, których dane przetwarza.
9. Administrator zarządza zmianami wpływającymi na prywatność. W tym celu wszelkie próby uruchamiania nowych projektów, inwestycji u administratora uwzględniają konieczność oceny wpływu zmiany na ochronę danych osobowych, analizę ryzyka, zapewnienie prywatności już na etapie projektowania zmiany, inwestycji czy na początku nowego projektu.

4. OBOWIĄZKI INFORMACYJNE PODSTAWY PRZETWARZANIA

1. Administrator określa zgodnie z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Administrator informuje osoby któych dane przetwarza o planowanej zmianie celu przetwarzania.
3. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych – chyba że takie działanie będzie wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.
4. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu jej danych osobowych, jeżeli może ono powodować duże ryzyko naruszenia praw lub wolności tej osoby.
5. Administrator dba o czytelnośc i styl przekazywania informacji i komunikacji z osobami,których dane przetwarza.
6. Administrator dokumentuje podstawy prawne przetwarzania danych osobowych
7. Administrator może w celu udokumentowania podstaw prawnych przetwarzania danych dla poszczególnych czynności przetwarzania utworzyć Rejestr.

5. POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

1. W przypadku zaistnienia sytuacji w której administrator ma podejrzenie, że mogło lub doszło do naruszenia zasad bezpieczeństwa danych osobowych w stopniu średnim lub wysokim administrator w ciągu 48h od powzięcia informacji o podejrzanym naruszeniu podejmuje stosowne działania w tym w szczególności:
   a) ustala zakres i przyczyny zagrożenia oraz ewentualne skutki niepożądanego działania;
   b) ustala osoby, które są odpowiedzialne za naruszenie;
   c) jeżeli uzna, że naruszenie jest poważne informuje o tym zdarzeniu osoby, których dane osobowe zostały naruszone;
   d) jeżeli uzna, że naruszenie jest poważne zgłasza naruszenie do UODO,
   e) ustala i wprowadza metody zmierzające do eliminacji podobnych zagrożeń w przyszłości.
2. W przypadku zaistenia sytuacji w której administrator uzna ponad wszelką wątpliwość, że naruszenie danych osobowych ma znikomy stopień ryzyka podejmuje działania eliminujące podobne zagrożenia w przyszłości.

6. POSTĘPOWANIE W PRZYPADKU ŻĄDAŃ OSÓB

1. ***Prawa osób trzecich.*** Realizując prawa osób trzecich, których dane dotyczą adminstrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku uzyskania

informacji o tym, iż wykonanie żądania o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (przykładowo: prawa związane z ochroną danych innych osób, prawo własności intelektualnej, tajemnicę handlową, dobra osobiste). Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeżeli taka osoba złożyła żądanie dotyczące jej praw.
3. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania zgodnie z art. 15 RODO.
5. ***Kopie danych.*** Administrator na żądanie wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Za wszelkie kolejne kopie, o które zwróci się osoba której dane dotyczą administrator ma prawo zgodnie z art. 15 RODO pobierać opłaty wynikające z kosztów administracyjnych. Administrator wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłąty za kolejne kopie danych. Cena kopi danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych i powinna być zgodnie z art. 15 RODO w rozsądnej wysokości.
6. ***Sprostowanie danych.*** Administrator dokonuje sprostowania nieprawidłowych danych na żadanie osoby. Administrator ma prawo odmówić sprostowania danych chyba, że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych administrator informuje osobę o odbiercach danych, na żądanie tej osoby.
7. ***Uzupełnianie danych.*** Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych jeżeli uzupełnienie było by niezgodne z celami przetwarzania danych.
8. ***Usunięcie danych.*** Na żądanie osoby administrator usuwa dane gdy: dane nie są niezbędne do celów dla których zostały zebrane albo ich przetwarzanie nie jest niezbędne w innych zgodnych z prawem celach;zgoda na ich przetważanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;dane były przetwarzane zgodnie z prawem;

7. PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych dopuszczalne jest przez administratora tylko,gdy:
   a) osoba której dane dotyczą wyrazi na to zgodę;
   b) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
   c) jest to niezbędne dla realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
   d) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
   e) jest to niezbędne dla wypełnienia prawnie usprawiedliwonych celów realizowanych przez administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osby, której dane dotyczą.
2. Za prawnie uzasadniony cel administrator uznaje w szczególności dochodzenie roszczeń z tytułu prowadzenia działalności gospodarczej.
3. Za prawnie uzasadniony cel administrator może również uznawać matketing bezpośredni własnych produktów i usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektronicznej należy stosować przepisy ustawy o świadczeniu usług drogą elektorniczną oraz ustawy prawo telekomunikacyjne.

8. ZASADY UDZIELANIA UPOWAŻNIENIEŃ DLA PRACOWNIKÓW

1. Podmiot przetwarzający jako pracodawca na podstawie art. 29 RODO nadaje upoważnienia pracownikom do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na danym stanowisku.
2. Upoważniona może być zarówno osoba zatrudniona na umowę o pracę, jak również osoba funkcjonująca w strukturze administrtora na podstawie umowy cywilnoprawnej.
3. Upoważniona może być osoba pełniąca rolę praktykanta, stażysty, a także osoba prowadząca działalność gospodarczą lub współpracująca z upoważnionym. Upoważniony musi być jednak zależny od administratora w zakresie decydowania o przetwarzaniu, a także działania w ramach przetwarzania.
4. ***Rodzaje i zakres udzielonych upoważnień.*** Administrator ustala poziomy upoważnienia pracowników obejmujące zakres uprawnień do przetwarzania danych osobowych

5. ***Odwołanie upoważnienia.*** Upoważnienie do przetwarzania danych osobowych może zostać odwołane w przypadku:kiedy pracownik jest w okresie wypowiedzenia/rozwiązania umowy o pracę;zmiany obowiązków pracownika, które nie wymagają przetwarzania danych osobowych;zmiany statusu pracownika, która wymusza odwołanie upoważnienia i podpisanie upoważnienia w innym zakresie;powzięcia informacji przez pracodawcę o wszczętym przeciwko pracownikowi postępowaniu karnym lub karnoskarbowym, jeżeli przemiotowe postępowanie może mieć wymierny wpływ na zaufanie pracodawcy do wykonywanych przez pracownika obowiązków;w każdym przypadku, jeżeli takie odwołanie będzie zgodne z polityką administratora; obowiązującymi przepisami prawa; przepisami RODO i w żaden sposób takie działanie nie wprowadzi ryzyka do naruszenia danych osobowych powierzonych administratorowi.

9. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

1. Administrator jeżeli uzna, że ryzyko przetwarzania danych osobowych wzrasta lub zachodzą inne prawdobodobne okoliczności naruszenia danych osobowych wprowadzi rejestr czynności przetwarzania danych osobowych.
2. Rejestr stanowi podstawową formę dokumentowania czynności przetwarzania danych ososbowych, pełni rolę mapy przetwarzania danych osobowych i jest jednym z kluczowych elemntów w jaki administrator może wskazać rozliczalność.
3. Rejestr inwentaryzuje i monitoruje sposób w jaki wykorzystywane są dane osobowe.
4. W rejestrze administrator odnotowuje, czynności które uznał za konieczne, w tym m.in:
   a) nazwę czynności;
   b) cel przetwarzania danych osobowych;
   c) opis kategorii osób;
   d) wskazanie podstawy prawnej przetwarzania/ celu prawnego przetwarzania;
   e) sposób zbiernia danych osobowych;
   f) ogólny opis technicznych i organizacyjnych środkó ochrony danych
5. W rejestrze można umieścić również kolumny nieobowiązkowe umieszcza się w nich dane w miarę potrzeb i możliwości, mając na uwadze, iż pełniejsz treść rejestru ułatwia zarządzanie danymi.

IV. PRZECHOWYWANIE DANYCH I PRAWA PODMIOTU KTÓREGO DANE SĄ PRZETWARZANE

1. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

1. Dane osobowe mogą być przechowywane przez cały okres zawartej na stałe umowy o współpracę do czasu przedawnienia ewentualnych roszczeń;
2. Dane marketingowe osobowe mogą być przechowywane do czasu wycofania zgody na przetwarzanie danych w tym celu, przy czym dane dotyczące uprzedniej zgody oraz operacji marketingowych zrealizowanych na tej podstawie wobec klienta będą przechowane w postaci archiwalnej przez 5 lat od momentu wycofania zgody (ograniczenie przetwarzania), dla potwierdzenia, że taka zgoda miała miejsce w przeszłości,
3. Dane osobowe dotyczące faktów i zdarzeń podlegających obowiązkom podatkowym lub ujęcia w odpowiednich księgach rachunkowych – przez okres wymagany postanowieniami ustaw: ordynacja podatkowa i ustawa o rachunkowości lub innych przepisów powszechnie obowiązujących,
4. Dane dotyczące realizacji praw osób, w tym praw konsumenta oraz praw wynikających z przepisów o ochronie danych osobowych - do czasu przedawnienia tych roszczeń lub do czasu zakończenia postępowań, dla których te dane są niezbędne do zapewnienia prawidłowości postępowania,
5. Dane osobowe zbierane w celu zapewnienia bezpieczeństwa serwisu – przez 5 lat od ich utrwalenia lub do zakończenia postępowania, jeśli te dane są niezbędne do zapewnienia prawidłowego przebiegu tego postępowania,

2. Chcielibyśmy poinformować, iż każdej osobie, której dane są przetwarzane przez Administratora w ramach prowadzenia Naszego Przedsiębiorstwa przysługuje:

1. prawo do:
2. dostępu do:
   a) swoich danych osobowych,
   b) sprostowania swoich danych osobowych,
   c) usunięcia swoich danych osobowych,
   d) ograniczenia przetwarzania swoich danych osobowych,
   e) sprzeciwu (w szczególności w przypadku przetwarzania danych w celach marketingowych) oraz prawo do przenoszenia danych w przypadkach określonych w RODO;
3. prawo cofnięcia zgody w dowolnym momencie, jednak bez wpływu na zgodność z prawem

przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

4. prawo wniesienia skargi do organu nadzoru, którym w Polsce jest **Prezes Urzędu Ochrony Danych Osobowych** z siedzibą w Warszawie, ul Stawki 2, skrzynka podawczą dostępna na stronie https://www.uodo.gov.pl/pl/p/kontakt, telefon kontaktowy (22) 531 03 00 – przed wniesieniem skargi proponujemy najpierw skontakotwać się z Administratorem w celu ugodowego rozwiązania problemu.

V. PODSUMOWANIE

1. Administrator zarządza zmianami mającymi wpływ na prywatność w taki sposób aby zapewnić odpowiednie bezpieczeństwo danych osobowych. Wszystkie zastosowane środki dostosowywane do aktualnie obowiazujacych przepisów prawa.
2. Polityka prywatności oraz regulaminy Administratora podlegą każdorazowej aktualizacji kiedy zachodzą okoliczności wymagające takiego działania.