POLITYKA

OCHRONY DANYCH

OSOBOWYCH

W: PR MANAGEMENT SEBASTIAN PAWEŁCZYK

Z SIEDZIBĄ W WOJKOWICACH

WOJKOWICE, DNIA 20.07.2018 R.

SPIS TREŚCI

SPIS ZAŁĄCZNIKÓW:

WPROWADZENIE

Niniejszy dokument zatytułowany „Polityka Ochrony Danych Osobowych" zwany dalej „Polityką", został sporządzony w celu wykazania, że SEBASTIAN PAWEŁCZYK prowadzący działalność gospodarczą pod firmą: PR MANAGEMENT Sebastian Pawełczyk (zwany dalej: „Administratorem danych") w ramach prowadzonego przedsiębiorstwa przetwarza i zabezpiecza dane osobowe zgodnie z wymogami prawa.

Polityka ma stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych u w/w Administratora danych. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu 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) (Dz. Urz. UE L 119, s.1).

Niniejsza Polityka zawiera:

1. opis zasad ochrony danych obowiązujących u Administratora,
2. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

Odpowiedzialnym za wdrożenie, utrzymanie i monitorowanie Polityki jest Administrator Danych – Sebastian Pawełczyk.

DEFINICJE TERMINÓW UŻYWANYCH W POLITYCE:

1. **Administrator Danych** –SEBASTIAN PAWEŁCZYK prowadzący działalność gospodarczą pod firmą PR MANAGEMENT Sebastian Pawełczyk z siedzibą w Wojkowicach przy ul. Długosza 15, NIP: 6252344417.
2. **Polityka** – Polityka Ochrony Danych Osobowych w: PR MANAGEMENT Sebastian Pawełczyk z dnia 20.07.2018 r.
3. **Dane osobowe -** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4. **Dane szczególnej kategorii –** dane wymienione w art. 9 ust 1 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;

5. **Osoba –** podmiot, którego dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
6. **System informatyczny -** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
7. **Zabezpieczenie danych w systemie informatycznym –** wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;
9. **Podmiot przetwarzający** – organizacja lub osoba, której Administrator powierzył przetwarzanie danych osobowych (np. zewnętrzna księgowość);
10. **Osoba upoważniona** – pracownik Administratora upoważniony pisemnie przez niego do przetwarzania danych osobowych;
11. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, udostępnianie, usuwanie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, niszczenie;
12. **Użytkownik systemu** – każda osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora, posiadająca unikalny identyfikator i hasło;
13. **Identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznych (Użytkownika systemu) w razie przetwarzania danych osobowych w takim systemie;
14. **Hasło -** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;
15. **RODO** – Rozporządzenie 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.

Rozdział I

Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych u Administratora niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka ma status dokumentu przeznaczonego do użytku wewnętrznego i może być udostępniona osobom trzecim tylko za zgodą Administratora.
4. Celem polityki jest wskazanie działań, które należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie zabezpieczenia danych osobowych.
5. Dla skutecznej realizacji Polityki Administrator danych zapewnia:
   - odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   - kontrolę i nadzór nad przetwarzaniem danych osobowych,
   - monitorowanie zastosowanych środków ochrony (m.in. poprzez monitorowanie działań dotyczących danych osobowych, naruszania zasad dostępu do danych, ochronę przed atakami zewnętrznymi oraz wewnętrznymi).
6. Zakres przedmiotowy Polityki obejmuje wszystkie zbiory danych osobowych przetwarzane u Administratora danych.
7. Polityka obowiązuje wszystkich pracowników Administratora oraz osoby pracujące na rzecz Administratora na podstawie umów cywilnoprawnych oraz na podstawie własnej działalności gospodarczej.

Rozdział II

OCHRONA DANYCH OSOBOWYCH – ZASADY, SYSTEM

1. Administrator stosuje następujące zasady ochrony danych osobowych:
   - w oparciu o podstawę prawną i zgodnie z prawem (legalizm),
   - rzetelnie i uczciwie (rzetelność),
   - w sposób przejrzysty dla osoby, której dotyczą (transparentność),
   - w konkretnych celach i nie „na zapas" (minimalizacja),
   - nie więcej niż potrzeba (adekwatność),
   - z dbałością o prawidłowość danych (prawidłowość),
   - nie dłużej niż potrzeba (czasowość),
   - zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo),
   - dokumentując spełnianie obowiązków w zakresie przetwarzania danych (rozliczalność).

2. System ochrony danych osobowych u Administratora składa się z następujących elementów:
   - analiza i identyfikacja okoliczności przetwarzania oraz ryzyka przetwarzania,
   - rejestr czynności przetwarzania danych osobowych,
   - podstawy prawne przetwarzania,
   - obsługa praw jednostki,
   - minimalizacja,
   - bezpieczeństwo,
   - powierzenie przetwarzania danych,
   - eksport danych,
   - projektowanie prywatności - *privacy by design*.

Rozdział III

SYSTEM OCHRONY DANYCH OSOBOWYCH – SZCZEGÓŁY

1. Analiza i identyfikacja okoliczności przetwarzania oraz ryzyka przetwarzania:

a) Polityka Ochrony Danych Osobowych opiera się na analizie i identyfikacji okoliczności przetwarzania oraz analizie ryzyka przetwarzania;

b) przez okoliczności przetwarzania rozumie się charakter, zakres, kontekst i cele przetwarzania danych osobowych;

c) charakter przetwarzania obejmuje:
   - rodzaj przetwarzanych danych, w tym czy dane przetwarzane są danymi szczególnej kategorii,
   - rodzaj nośników, na których dane są przetwarzane, w tym czy dane są przetwarzane w systemie informatycznym czy w formie papierowej,
   - podstawę prawną przetwarzania danych osobowych,
   - częstotliwość przetwarzania danych osobowych, w tym czy dane przetwarzane są w sposób ciągły, systematyczny lub incydentalny,
   - stwierdzenie czy przetwarzane dane pochodzą bezpośrednio od osób, których dotyczą, czy od innych osób.

d) zakres przetwarzania obejmuje konkretne czynności przetwarzania, które są wykonywane

e) kontekst przetwarzania obejmuje umiejscowienie przetwarzania w czasie i przestrzeni; przy definiowaniu kontekstu przetwarzania bierze się pod uwagę konkretne otoczenie i środowisko przetwarzania danych, takie jak miejsce przetwarzania oraz fizyczne i techniczne sposoby zabezpieczenia przetwarzania - czynniki te muszą mieć wpływ na czynności przetwarzania

f) cele przetwarzania danych są konkretne i odnoszą się do podstawy prawnej przetwarzania; przy definiowaniu celów przetwarzania bierze się pod uwagę:
   - czy przetwarzanie jest niezbędne do wypełnienia obowiązku ciążącego na administratorze,
   - czy cel przetwarzania danych może zmienić się względem celu w jakim dane zostały zebrane oraz czy w związku ze zmianą celu przetwarzania zmienia się podstawa prawna przetwarzania;

g) Analiza i ocena ryzyka obejmuje szacowanie prawdopodobieństwa wystąpienia zdarzenia naruszającego prawa osób, których dane są przetwarzane oraz określeniu istotności efektów takiego zdarzenia. Każdemu zidentyfikowanemu ryzyku przypisuje się skalę liczbową lub jakościową np. niski – średni - wysoki;

h) wybór formy postępowania z ryzykiem obejmuje: obniżenie poziomu ryzyka poprzez zastosowanie odpowiednich środków organizacyjnych lub faktycznych (np. szkolenia pracowników), unikanie ryzyka (np. poprzez niewdrażanie określonych projektów, które

wymagają przetwarzania danych wrażliwych), lub przeniesienie ryzyka (np. poprzez zawarcie odpowiednich klauzul w umowach z kontrahentami);

i) Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

2. Rejestr czynności przetwarzania danych osobowych (RCPD):

a) RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych i jest jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności,
b) RCPD inwentaryzuje i monitoruje sposób, w jaki wykorzystuje się u Administratora dane osobowe,
c) w rejestrze dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru odnotowuje się co najmniej: nazwę czynności, cel przetwarzania, opis kategorii danych, podstawę prawną przetwarzania danych, sposób zbierania danych, opis kategorii odbiorców danych, informację o przekazaniu danych poza EU/EOG, ogólny opis technicznych i organizacyjnych środków ochrony danych, planowany termin usunięcia danych
d) wzór Rejestru stanowi załącznik nr 1 do Polityki – **„Wzór Rejestru Czynności Przetwarzania Danych".**

3. Podstawy prawne przetwarzania:

a) Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania
b) Administrator dokumentuje w Rejestrze (RCPD) podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania
c) Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację zgody osoby na przetwarzanie jej konkretnych danych osobowych w konkretnym celu, jak również rejestrację cofnięcia zgody, sprzeciwu, ograniczenia, itp.
d) Administrator uzyskuje zgodę osoby na przetwarzanie danych osobowych za pomocą **„Klauzuli zgody na przetwarzanie danych osobowych"**, której wzór stanowiącej załącznik nr 2 do Polityki"
e) każdy uczestnik procesu przetwarzania danych osobowych zna podstawę prawną, na jakiej dokonywana jest konkretna czynności przetwarzania

4. Obsługa praw jednostki:

<u>Sposób obsługi praw jednostki - obowiązki informacyjne</u>

a) Administrator samodzielnie lub poprzez upoważnionych w tym zakresie pracowników spełnia obowiązki informacyjne względem osób, których dane przetwarza poprzez:

- przekazanie informacji prawem wymaganych przy zbieraniu danych;
- przekazywanie informacji przy użyciu klauzuli informacyjnej, której wzór stanowi załącznik nr 3 do Polityki - **„Klauzula informacyjna";**
- dbałość o czytelność i styl przekazywanych informacji;
- podejmowanie działań mających na celu ułatwienie zapoznania się z informacjami dotyczącymi przetwarzanych danych osobowych, w tym m.in. zamieszczenie na stronie internetowej Klauzuli Informacyjnej lub odwołań (linków) do w/w informacji;

b) dane osobowe przetwarzane przez Administratora nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu
c) Administrator informuje osobę o planowanej zmianie celu przetwarzania danych osobowych oraz przed uchyleniem ograniczenia przetwarzania
d) Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby
e) Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień oraz żądań osób

Sposób obsługi praw jednostki - Żądania osób

a) Administrator zapewnia obsługę praw osób, które wynikają z Rozdziału III RODO, realizując otrzymane w tym zakresie żądania ustne lub pisemne niezwłocznie, **nie dłużej niż do 1 miesiąca** licząc od dnia złożenia żądania,
b) Administrator na żądanie osób, bezzwłocznie udziela informacji dotyczących przetwarzania danych osobowych, a które to wynikają z Klauzuli Informacyjnej;
c) Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych;
d) realizując prawa osób, których dane dotyczą, Administrator wprowadza gwarancje ochrony praw i wolności osób trzecich; w szczególności w przypadku powzięcia wiarygodnej informacji o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób, Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienie żądaniu;
e) Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby oraz uzupełnia dane i aktualizuje dane na żądanie osoby; Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie przetwarza danych, które są dla niego zbędne);
f) na żądanie osoby Administrator usuwa dane, w przypadkach wskazanych w art. 17 RODO;

g) Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, w przypadkach wskazanych w art. 18 RODO;
h) jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane są przetwarzane przez Administratora w oparciu o jego uzasadniony interes lub o powierzone mu zadanie w interesie publicznym, Administrator uwzględni sprzeciw i ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw lub podstawy do ustalenia, dochodzenia lub obrony roszczeń;
i) jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego, Administrator uwzględnia sprzeciw i zaprzestaje takiego przetwarzania.

5. Minimalizacja:
a) Administrator dba o minimalizację przetwarzania danych pod kątem adekwatności zbieranych danych do celów przetwarzania;
b) Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności na etapie Analizy i identyfikacji okoliczności przetwarzania oraz ryzyka przetwarzania (opisanych w Rozdziale III pkt 1)
c) Administrator stosuje ograniczenia dostępu do danych osobowych: organizacyjne oraz techniczne. Szczegółowe informacje dotyczące ograniczeń w dostępnie do danych osobowych znajdują się w Rozdziale IV poniżej;
d) Administrator dba o minimalizację przetwarzania danych pod kątem czasu przechowywania danych i w tym celu dokonuje weryfikacji dalszej przydatności przetwarzanych danych osobowych; dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych Administratora, jak też z dokumentacji papierowej, a po zakończeniu procesu archiwizacji są niszczone, w sposób uniemożliwiający ich odzyskanie tj.:
   - dokumentacja związana z realizacją umowy/zamówienia przechowywana jest w aktach podręcznych przez **czas realizacji umowy**, a następnie jest archiwizowana do momentu **przedawnienia roszczeń z tytułu zawartej umowy**;
   - dokumentacja związana ze zgłoszonymi skargami, reklamacjami, gwarancjami przechowywana jest w aktach podręcznych przez czas rozpatrywania złożonego wniosku, a następnie jest archiwizowana **przez okres 1 roku** licząc od dnia zakończenia w/w postępowania;
   - dokumentacja księgowa znajduje się u procesora **przez okres 1 roku**, następnie jest przekazywana do Administratora, gdzie jest przechowywana w archiwum **przez okres 5 lat**, zgodnie z wymaganiami przepisów prawa;

- dokumentacja związana z dochodzeniem roszczeń przechowywana jest **do czasu zakończenia postępowań** windykacyjnych, sądowych oraz egzekucyjnych;
- dokumentacja kadrowa przechowywana jest w aktach podręcznych **do czasu zakończenia stosunku pracy**, a następnie jest archiwizowana **przez okres 50 lat** licząc od momentu ustania zatrudnienia;
- zgody osób dotyczące przetwarzania danych osobowych przechowywane **są do czasu ich cofnięcia**;
- zapisy z monitoringu przechowywane są **przez okres max. 30 dni** licząc od dnia rejestracji obrazu;

6. Bezpieczeństwo:

a) szczególną uwagę Administrator zwraca na elementy zarządzania, które mają istotny wpływ na bezpieczeństwo danych rozumiane jako ochrona przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

b) Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych; w tym celu przeprowadza analizy ryzyka dla czynności przetwarzania danych lub kategorii;

c) Administrator podczas tworzenia niniejszej Polityki nie przeprowadził oceny skutków przetwarzania dla ochrony danych, gdyż charakter, zakres, kontekst i cele przetwarzania danych osobowych nie wskazują na duże prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób trzecich; Administrator nie przetwarza danych szczególnych kategorii;

d) Administrator stosuje zróżnicowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Szczegółowe informacje dotyczące zastosowanych środków bezpieczeństwa znajdują się w Rozdziale IV poniżej;

e) Administrator zarządza incydentami – stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych. Szczegółowe informacje dotyczące zarządzania incydentami znajdują się w Rozdziale V poniżej.

7. Powierzenie przetwarzania danych oraz ujawnianie danych innym podmiotom:

a) ujawnienie danych osobowych uprawnionym na podstawie przepisów prawa organom władzy publicznej w ramach prowadzonego przez te organy postępowania nie wymaga informowania o ujawnieniu osoby, której dane dotyczą; ujawnienie danych następuje po wskazaniu przez organ przepisu uprawniającego do ujawnienia danych oraz podstawy

prawnej przetwarzania danych osobowych, a takie ujawnienie rejestrowane jest w **Rejestr udostępnień, którego wzór stanowi załącznik nr 4;**

b) ujawnianie danych podmiotom zewnętrznym innym niż opisanym powyżej jest dopuszczalne jedynie wtedy, jeżeli podstawa prawna przetwarzania i cel przetwarzania dopuszczają ujawnienie danych oraz jeżeli osoba została poinformowana o możliwych odbiorcach lub ich kategoriach zgodnie z art. 13 RODO;

c) w celu zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków w zakresie ochrony danych osobowych spoczywających na Administratorze, dokonuje on weryfikacji podmiotów, którym ma zostać powierzone przetwarzanie danych osobowych pod kątem stosowanych przez nich środków organizacyjnych i technicznych zapewniających bezpieczeństwo przetwarzania danych;

d) Administrator powierzając przetwarzanie danych osobowych zawiera z podmiotem **„Umowę powierzenia przetwarzania danych"** której wzór stanowi załącznik nr 5 do Polityki. Administrator prowadzi rejestr zawartych umów powierzenia. **Wzór rejestru stanowi załącznik nr 6 do Polityki.**

8. Eksport danych:

Administrator nie eksportuje danych do państwa trzeciego lub organizacji międzynarodowej.

9. Projektowanie prywatności – *Privacy by design*:

a) Administrator zarządza zmianami mającymi wpływ na prywatność w taki sposób, aby zapewnić odpowiednie bezpieczeństwo danych osobowych oraz minimalizację ich przetwarzania;

b) procedury uruchamiania nowych projektów i inwestycji u Administratora uwzględniają konieczność oceny wpływu zmiany na ochronę danych osobowych, analizę ryzyka, a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

ROZDZIAŁ IV.
ŚRODKI NIEZBĘDNE DO ZACHOWANIA BEZPIECZEŃSTWA DANYCH

Administrator stosuje zróżnicowane środki zapewniające ochronę przetwarzanych danych osobowych. Stosowane środki organizacyjno-techniczne są wynikiem przeprowadzonego postępowania z ryzykiem obejmującego jego analizę oraz wybór sposobu postępowania i dzielą się na:

1. Przetwarzanie danych osobowych na podstawie upoważnienia od Administratora:

a) każdy pracownik Administratora jest zobowiązany do zachowania poufności informacji uzyskanych w związku z wykonywaniem czynności pracowniczych;
b) każdy pracownik Administratora przetwarzający dane osobowe musi posiadać upoważnienie do przetwarzania danych osobowych stanowiące polecenie Administratora w rozumieniu art. 29 RODO oraz 32 ust. 4 RODO; upoważnienie zawiera wszystkie wymagane prawem informacje oraz ewentualny poziom dostępu do systemu informatycznego Administratora;
c) nadanie upoważnień do przetwarzania danych osobowych odbywa się na podstawie załącznika nr 7 do Polityki **– „Upoważnienie do przetwarzania danych osobowych";**
d) upoważnienie połączone jest z deklaracją pracownika o zachowaniu w tajemnicy danych osobowych, sposobów ich zabezpieczania, jak również zapoznania się z treścią Polityki;
e) najpóźniej w ostatnim dniu pracy anuluje się upoważnienie poprzez dokonanie odpowiedniej adnotacji w dokumencie upoważnienia;
f) upoważnienia przechowuje się w miejscu, w którym przechowywana jest dokumentacja kadrowa;
g) upoważnieni pracownicy zachowują odpowiednie środki bezpieczeństwa w zakresie przetwarzania danych osobowych w tym m.in.:
   - odpowiadają za faktyczne przetwarzanie danych osobowych, które jest niezbędne do realizacji ich zadań wynikających z indywidualnego zakresu obowiązków oraz zakresu procesów przetwarzania danych osobowych, który wyznaczył Administrator;
   - przetwarzają tylko te dane, których przetwarzanie jest niezbędne ze względu na realizację zleconych zadań;
   - zachowują najwyższy stopień staranności przy wykonywaniu czynności przetwarzania;
   - przetwarzają dane osobowe wyłącznie w zakresie ustalonym w upoważnieniu i tylko w celu wykonywania obowiązków;
   - zachowują w tajemnicy dane osobowe, które zostały im ujawnione w trakcie wykonywania obowiązków;

- chronią dane osobowe, które przetwarzają przed nieuprawnionym ujawnieniem, modyfikacją czy zniszczeniem;
- korzystają z zasobów informatycznych w sposób zgodny z niniejszą Polityką Ochrony Danych Osobowych oraz instrukcjami obsługi urządzeń;
- niezwłocznie informują Administratora o wszelkich nieprawidłowościach związanych z przetwarzaniem danych osobowych;
- wyczerpująco i skrupulatnie informują osoby, której dane są przetwarzane o okolicznościach przetwarzania, korzystając w tym celu z obowiązującej u Administratora Klauzuli informacyjnej (tzw. obowiązek informacyjny);
- dokumentują czynności związane z przetwarzaniem danych osobowych zgodnie z niniejszą Polityką Ochrony Danych Osobowych i załącznikami;
- w trybie natychmiastowym informują Administratora o każdej sytuacji, która może stanowić naruszenie bezpieczeństwa danych osobowych.

2. Przetwarzanie danych osobowych w wyznaczonych miejscach i w określony sposób:

a) Administrator przetwarza dane osobowe w pomieszczeniach znajdujących się w Wojkowicach przy ul. Długosza 15;
b) dostęp do pomieszczeń w których odbywa się przetwarzanie danych osobowych mają klienci oraz pracownicy; w związku z powyższym dokumenty papierowe oraz inne nośniki informacji zawierające dane osobowe są przechowywane w szafach zamykanych na klucz (pomieszczenie również zamykane są na klucz); komputer/y są ustawione w taki sposób, aby nikt z osób postronnych nie widział treści znajdujących się na ekranach monitorów;
c) Administrator w pomieszczeniu zamykanym na klucz znajdującym się w siedzibie firmy prowadzi archiwum, w którym przechowywana jest dokumentacja zawierająca dane osobowe; dokumentacja znajduje się w oddzielnych szafach, zabezpieczonych kluczem, do których dostęp ma tylko Administrator oraz osoby upoważnione;
d) po zakończeniu pracy w pomieszczeniach przetwarzania danych osobowych obowiązkowo sprawdza się prawidłowość zamknięcia szaf, okien oraz drzwi wejściowych;
e) poza czasem pracy, szafy i szuflady pozostają zamknięte; pomieszczenia można otworzyć tylko w celu sprzątania, konserwacji lub w innych celach związanych z zachowaniem bezpieczeństwa osób lub mienia; klucze do zamkniętych szaf składowane są w jednym miejscu tj. w oddzielnej szafce zamykanej na klucz lub sejfie do których dostęp ma Administrator oraz upoważnieni pracownicy; klucze są wydawane tylko upoważnionym pracownikom i tylko na czas pracy;
f) pomieszczenia objęte są monitoringiem wizyjnym;

g) dokumenty papierowe zawierające dane osobowe są chronione przed ich fizycznym uszkodzeniem lub zniszczeniem;
h) Administrator rozróżnia 2 rodzaje dokumentów zawierające dane osobowe tj. dokumenty robocze oraz dokumenty archiwalne; dokumenty robocze niezbędne są w bieżącej pracy, natomiast dokumenty archiwalne, to dokumenty które nie są niezbędne do wykonywania bieżącej pracy, ale z uwagi na swoją przydatność przechowywane są przez odpowiedni okres w archiwum ;
i) każdy dokument zawierający dane osobowe mający charakter dokumentu roboczego jest na koniec pracy chowany w szafce zamykanej na klucz; podczas pracy dokument jest umieszczany w taki sposób, aby osoby postronne nie mogły zapoznać się z jego treścią;
j) każdy dokument zawierający dane osobowe mający charakter dokumentu roboczego jest po okresie przydatności brakowany w niszczarce lub przeznaczony do zniszczenia (powyższe nie dotyczy dokumentów otrzymujących rangę dokumentu archiwalnego);
k) stosuje się zasadę tzw. czystego biurka i czystego pulpitu stacji roboczej;
l) w przypadku przenoszenia dokumentów zawierających dane osobowe pomiędzy pomieszczeniami przetwarzania danych, każdorazowo zabezpiecza się je przed dostępem osób nieupoważnionych oraz przed ich utratą lub zniszczeniem.

3. Przetwarzanie danych osobowych przy wykorzystaniu systemu informatycznego:

a) w działalności Administratora wykorzystywane są komputery stacjonarne oraz urządzenia przenośne tj. nośniki zewnętrzne, smartfony, laptopy;
b) dostęp do komputerów, nośników zewnętrznych, na których znajdują się dane osobowe ma tylko Administrator oraz upoważnieni pracownicy;
c) uprawnieni użytkownicy systemu informatycznego posiadają identyfikator (login) oraz hasło o odpowiedniej jakości (hasło zawiera min. 6 znaków, w tym min. 1 wielką literę, 1 małą literę, 1 cyfrę); zmiana hasła następuje co 6 miesięcy;
d) zabronione jest udostępnianie hasła do systemu informatycznego innym osobom;
e) w urządzeniach stosowane jest oprogramowanie antywirusowe, a w czasie rzeczywistym sprawdzane są wszystkie przychodzące i wychodzące pliki;
f) w urządzeniach systemu informatycznego stosowana jest profilaktyka antywirusowa;
g) urządzenia nie są pozostawiane bez nadzoru oraz nie przekazuje się ich do korzystania nieupoważnionym osobom;
h) stosowana jest procedura wykonywania kopii zapasowych danych zawierających dane osobowe; kopie zapasowe wykonuje się na dyskach sieciowych;
i) połączenia z sieci lokalnej z siecią publiczną są wykonywane za pośrednictwem systemów firewall;

j) korzystanie z zasobów sieci lokalnej jest możliwe wyłącznie w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych;
k) stosuje się blokadę komputera w przypadku opuszczenia stanowiska pracy lub dłuższej nieaktywności użytkownika;
l) Administrator zapewnia możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
m) wszelkie zmiany w zakresie stosowanego oprogramowania komputerowego możliwe są tylko przez osoby posiadające osobne upoważnienie od Administratora;
n) w ramach serwisu internetowego Administrator stosuje zabezpieczenia w postaci posiadania certyfikatu SSL;
o) zbiorcze listy zawierające dane osobowe klientów sklepu, użytkowników sklep internetowego są zabezpieczone poprzez szyfrowani oraz pseudonimizację.

ROZDZIAŁ V

ZARZĄDZANIE INCYDENTAMI

1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych Administrator uważa m.in.:

a) naruszenie bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe,

b) udostępnienie lub umożliwienie udostępnienia danych osobom lub podmiotom nieupoważnionym,

c) zaniechanie, choćby nieumyślnie, dopełnienia obowiązku zapewnienia danym osobowym ochrony,

d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,

e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,

f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych,

g) naruszenie praw osób, których dane są przetwarzane.

2. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło spowodować ryzyko naruszenia praw lub wolności osób fizycznych. Jednocześnie Administrator sporządza raport z naruszenia ochrony danych osobowych. Wzór raportu stanowi załącznik nr 8 do Polityki – **„Wzór raportu z naruszenia ochrony danych osobowych".**
3. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia. Wzór zgłoszenia stanowi załącznik nr 9 do Polityki – **„Wzór zgłoszenia incydentu naruszenia ochrony danych".**
4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
5. Administrator prowadzi **„Rejestr naruszeń ochrony danych osobowych",** którego wzór stanowi załącznik nr 10 do Polityki.
6. W celu usystematyzowania działań Administratora podejmowanych w przypadku zaistnienia incydentów naruszeń ochrony danych osobowych, Administrator wprowadził schemat graficzny przedstawiający niezbędne działania. Schemat stanowi załącznik nr 11 do Polityki – **„Schemat postępowania w przypadku naruszenia ochrony danych osobowych".**

ROZDZIAŁ VI

POSTANOWIENIA KOŃCOWE

1. Załączniki do Polityki Ochrony Danych Osobowych są jej integralną częścią. Na strukturę dokumentów związanych z ochroną danych osobowych składa się Polityka Ochrony Danych jako dokument główny, także załączone do niej procedury i wzory.
2. Wszelkie niejasności związane z rozumieniem załączników należy rozpatrywać w zgodności z Polityką Ochrony Danych Osobowych.

ZAŁĄCZNIK NR 1

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH

NAZWA: CZYNNOŚCI PRZETWARZANIA ZWIĄZANE Z:

1. **Administrator Danych:**
2. **Dane Współadministratora:**
3. **Cel przetwarzania danych w zbiorze:**
4. **Opis kategorii osób, których dane są przetwarzane w zbiorze:**
5. **Podstawa prawna przetwarzania danych:**
6. **Sposób zbierania danych:**
7. **Zakres danych przetwarzanych w zbiorze:**
8. **Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione:**
9. **Nazwa Państwa trzeciego do którego dane są przekazywane**:
10. **Planowane terminy usunięcia poszczególnych kategorii danych:**
11. **Nazwa systemu lub oprogramowania:**
12. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:**

_____

podpis Administratora

ZAŁĄCZNIK NR 2

WZÓR KLAUZULI ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

KLAUZULA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

Czy zgadzasz się na przetwarzanie Twoich danych osobowych takich jak:

a. Imię ……..…

b. Nazwisko……

c. Adres ……..

d. NIP……...…..

e. nr telefonu……

f. adres e-mail ……

przez: SEBASTIAN PAWEŁCZYK prowadzący działalność gospodarczą pod firmą PR MANAGEMENT Sebastian Pawełczyk z siedzibą w Wojkowicach przy ul. Długosza 15, NIP: 6252344417 w celach marketingowych za pomocą środków porozumiewania się na odległość.

[ ] NIE [ ] TAK

Podpis Podpis

…… ……...

ZAŁĄCZNIK NR 3

WZÓR KLAUZULI INFORMACYJNEJ

Szanowni Państwo,

od 25 maja 2018 r. obowiązuje Ogólne Rozporządzenie z dnia 27 kwietnia 2016 r. o ochronie danych osobowych (dalej „RODO"). W związku z powyższym przedstawiamy Państwu niniejszą informację, dzięki której dowiecie się, jak przetwarzamy Państwa dane osobowe.

ADMINISTRATOR DANYCH:

Administratorem Państwa danych osobowych jest SEBASTIAN PAWEŁCZYK prowadzący działalność gospodarczą pod firmą PR MANAGEMENT Sebastian Pawełczyk z siedzibą w Wojkowicach przy ul. Długosza 15, NIP: 6252344417.

KONTAKT Z ADMINISTRATOREM:

W zakresie przetwarzania danych osobowych z Administratorem można kontaktować się:

- pisemnie na adres siedziby tj. PR MANAGEMENT Sebastian Pawełczyk z siedzibą w Wojkowicach(42-580) przy ul. Długosza 15;
- poprzez e-mail: BIURO@PRMANAGEMENT.PL
- telefonicznie pod numerem telefonu: 791948747.

CEL PRZETWARZANIA DANYCH OSOBOWYCH, PODSTAWA PRZETWARZANIA ORAZ CZAS PRZETWARZANIA:

Państwa dane osobowe przetwarzane będą w celach:

- zawarcia i wykonania umowy (w tym kontaktowanie się z klientem w związku z realizacją umowy) – podstawą prawną przetwarzania jest art. 6 ust. 1 lit. b RODO; czas przetwarzania: przez okres trwania umowy i do czasu przedawnienia roszczeń z tytułu zawartej umowy;
- rozpatrywania skarg i reklamacji - podstawą prawną przetwarzania jest art. 6 ust. 1 lit. c RODO; czas przetwarzania: przez okres 1 roku po upływnie terminu rękojmi, gwarancji lub rozliczeniu reklamacji;
- dochodzenia roszczeń związanych z zawartą umową – podstawą prawną przetwarzania jest art. 6 ust. 1 lit. f RODO tj. realizacja prawnie uzasadnionego interesu Administratora, rozumianego jako windykacja należności, prowadzenie postępowań sądowych oraz egzekucyjnych; czas przetwarzania: do czasu zakończenia postępowań sądowych i egzekucyjnych;
- archiwalnych (dowodowych) – podstawą prawną przetwarzania jest art. 6 ust. 1 lit. c RODO; czas przetwarzania: do momentu wygaśnięcia obowiązku przechowywania danych

wynikającego z przepisów prawa, a w szczególności obowiązku przetwarzania dokumentów księgowych;

- statystycznych – podstawą prawną przetwarzania jest art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu rozumianego jako zbieranie informacji o jakości naszej obsługi oraz poziomu zadowolenia klientów w celu poprawy naszej działalności; do czasu posiadania dodatkowej innej podstawy prawnej przetwarzania;
- oferowania produktów i usług produktów bez wykorzystania środków komunikacji elektronicznej - podstawą przetwarzania jest art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu rozumianego jako reklamowania swojej działalności; czas przetwarzania: do czasu wniesienia sprzeciwu;
- oferowania produktów i usług produktów z wykorzystaniem środków komunikacji elektronicznej - podstawą przetwarzania jest art. 6 ust. 1 lit. a RODO oraz art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu rozumianego jako reklamowania swojej działalności przy wykorzystaniu adresów e-mail, numerów telefonu; czas przetwarzania: do czasu cofnięcia zgody lub zgłoszenia sprzeciwu;
- obsługi zapytań składanych przy wykorzystaniu formularza kontaktowego – podstawą przetwarzania jest art. 6 ust. 1 lit. f RODO realizacja prawnie uzasadnionego interesu rozumianego jako utrzymywanie kontaktu z potencjalnym klientem; czas przetwarzania: do czasu udzielenia odpowiedzi na zapytanie.

UDOSTĘPNIENIE DANYCH OSOBOWYCH:

Państwa dane osobowe mogą być przekazane innym podmiotom, z którymi współpracujemy, w szczególności:

- podmiotom prowadzącym działalność pocztową, kurierską;
- podmiotom umożliwiającym nam dokonywanie zdalnych operacji płatniczych;
- organom państwowym lub innym podmiotom uprawnionym na podstawie przepisów prawa, celem wykonania ciążących na nas obowiązków (Urząd Skarbowy, PIP, ZUS),
- podmiotom z nami współpracującymi, świadczącym dla nas usługi na podstawie umów zlecenia tj. firmie księgowej, obsłudze IT, przy czym podmioty te przetwarzają dane na podstawie umowy z Administratorem i wyłącznie zgodnie z poleceniem Administratora;

DOBROWOLNOŚĆ PODANIA DANYCH OSOBOWYCH:

Podanie danych jest dobrowolne, ale niezbędne do zawarcia i realizacji umowy. W przypadku niepodania danych niemożliwe będzie zawarcie umowy i realizacja zlecenia.

PRAWA ZWIĄZANE Z PRZETWARZANYMI DANYMI OSOBOWYMI:

W związku z przetwarzanymi danymi osobowymi przysługują Państwu następujące prawa:

- dostęp do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania;
- wniesienie sprzeciwu;
- przenoszenia danych;
- wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych;
- cofnięcia zgody na przetwarzanie danych osobowych w dowolnym momencie, gdy podstawą przetwarzania jest udzielona przez Państwa zgoda (wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano przed wycofaniem zgody).

PRAWO DO SPRZECIWU:

W każdej chwili przysługuje Państwu prawo do wniesienia sprzeciwu wobec przetwarzania danych na podstawie uzasadnionego interesu, ale z wyłączeniem marketingu bezpośredniego. Przestaniemy przetwarzać Państwa dane w tym celu, chyba że będziemy w stanie wykazać, że w stosunku do tych danych istnieją dla nas ważne prawnie uzasadnione podstawy, które są nadrzędne wobec Państwa interesów, praw i wolności lub Państwa dane będą nam niezbędne do ewentualnego ustalenia, dochodzenia lub obrony roszczeń;
W każdej chwili przysługuje Państwu prawo do wniesienia sprzeciwu wobec przetwarzania danych w celu prowadzenia marketingu bezpośredniego. Zaprzestaniemy przetwarzania danych w tym celu, jeżeli skorzystają Państwo z tego prawa.

ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI:

Państwa dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

W ramach wykonywanych czynności korzystamy z plików cookies w ten sposób, że obserwujemy i analizujemy ruch na naszych stronach, jak również podejmujemy działania remarketingowe, jednakże w ramach tych czynności nie przetwarzamy danych osobowych w rozumieniu RODO.

PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO:

Państwa dane nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;

ZAŁĄCZNIK NR 4

WZÓR REJESTRU UDOSTĘPNIEŃ

L.p.	Podmiot, któremu udostępniono dane	Data udostę-pnienia	Podstawa prawna udostę-pnienia	Zakres udostępnionych danych	Podpis Administratora

ZAŁĄCZNIK NR 5

WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych

zawarta w Czeladzi, w dniu _____ pomiędzy:
SEBASTIANEM PAWEŁCZYKIEM prowadzący działalność gospodarczą pod firmą: PR MANAGEMENT Sebastian Pawełczyk z siedzibą w Wojkowicach przy ul. Długosza 15, posługującym się NIP: 6252344417.
zwanym dalej **„Administratorem"**

a

_____

zwaną dalej **„Podmiotem przetwarzającym"**

zwanymi każdą z osobna w dalszej części Umowy **„Stroną",** a łącznie **„Stronami".**
o następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 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; Dz. Urz. UE L 119, s.1) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot Przetwarzający zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia, jak również oświadcza, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

§ 2

Cel, zakres przetwarzania powierzonych danych osobowych

1. Podmiot przetwarzający będzie przetwarzał powierzone dane _____ w postaci: _____
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy _____ z dnia _____ i wyłącznie w zakresie, jaki jest niezbędny do realizacji tego celu.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
2. Podmiot przetwarzający zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Zleceniobiorca oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
4. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
5. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.
7. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej umowie oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.

8. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków w zakresie ochrony danych.
9. Podmiot przetwarzający oświadcza, ze nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy – EOG).

§ 4

Odpowiedzialność Podmiotu przetwarzającego

Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym

§ 5

Rozwiązanie Umowy

1. Niniejsza umowa powierzenia przetwarzania danych osobowych obowiązuje na czas trwania umowy, o której mowa w § 2 ust. 2.
2. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe niezgodnie z umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 6

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, a by środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych, w tym w szczególności danych

osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§ 7

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W zakresie nieuregulowanym niniejszą Umową zastosowanie mają przepisy Kodeksu cywilnego.
3. W przypadku gdy niniejsza Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

_____ _____

Administrator Podmiot przetwarzający

ZAŁACZNIK NR 6

WZÓR REJESTRU ZAWARYCH UMÓW POWIERZENIA

L.p.	Podmiot przetwarzający / Podmiot powierzający	Cel przetwarzania	Termin obowiązywania	Podstawa prawna przetwarzania	Podpis Administratora

ZAŁĄCZNIK NR 7

WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Czeladź, dn. _____

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Numer: _____

Na podstawie art. 29 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) (Dz. Urz. UE L 119, s.1) – dalej RODO upoważniam:

Pana/ią _____, zam. _____

w okresie od _____ **do** odwołania,

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowany stanowisku _____**. Niniejsze upoważnienie obejmuje uprawnienie do przetwarzania następujących danych osobowych** _____

Nadano identyfikator do Systemu Informatycznego: _____

Jednocześnie zobowiązuję Pana/ią do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz przepisami prawa, w tym RODO oraz Polityką Ochrony Danych Osobowych obowiązującą u Administratora. Informuję, również że dane osobowe, do których przetwarzania upoważnia niniejszy dokument oraz sposoby ich zabezpieczenia stanowią tajemnicę służbową w rozumieniu art. 266 §1 kodeksu karnego.

Ponadto upoważniam Pana/ią do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych u Administratora.

_____

podpis Administratora

Data wygaśnięcia: _____

ZOBOWIĄZANIE OSOBY UPOWAŻNIONEJ

Oświadczam, że zapoznałam/-em się z zakresem swojego upoważnienia, jak również z Polityką Ochrony Danych Osobowych, służącymi do ochrony danych osobowych u Administratora.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobu ich zabezpieczeń, także po ustaniu stosunku pracy oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.

_____

data i podpis osoby upoważnionej

ZAŁĄCZNIK NR 8

WZÓR RAPORTU Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

_____dn._____

Raport z naruszenia ochrony danych	
Lokalizacja oraz dzień naruszenia.	
Kategoria i przybliżona liczba osób, których dane dotyczą oraz wpisów danych osobowych, których dotyczy naruszenie.	
Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe).	
Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu.	
Podjęte działania.	
Wstępna ocena przyczyn wystąpienia naruszenia	
Postępowanie wyjaśniające i naprawcze	
Możliwe konsekwencje naruszenia ochrony danych osobowych.	

_____ _____

(data i podpis pracownika) (data i podpis Administratora)

ZAŁĄCZNIK NR 9

WZÓR ZGŁOSZENIA INCYDENTU NARUSZENIA DANYCH OSOBOWYCH

_____, dn. _____

Prezes Urzędu Ochrony Danych Osobowych

ZGŁOSZENIE INCYDENTU NARUSZENIA DANYCH OSOBOWYCH

Działając na podstawie art. 33 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, Dz. Urz. UE L 119, s.1), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych	
Miejsce i dzień naruszenia	
Kategoria i przybliżona liczna osób, których dane dotyczą	
Kategoria i przybliżona liczba wpisów danych osobowych, których dane dotyczą	
Opis charakteru naruszeń ochrony danych, określenie okoliczności towarzyszących naruszeniu oraz przyczyna wystąpienia naruszenia	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

ZAŁĄCZNIK NR 10

WZÓR REJESTRU NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

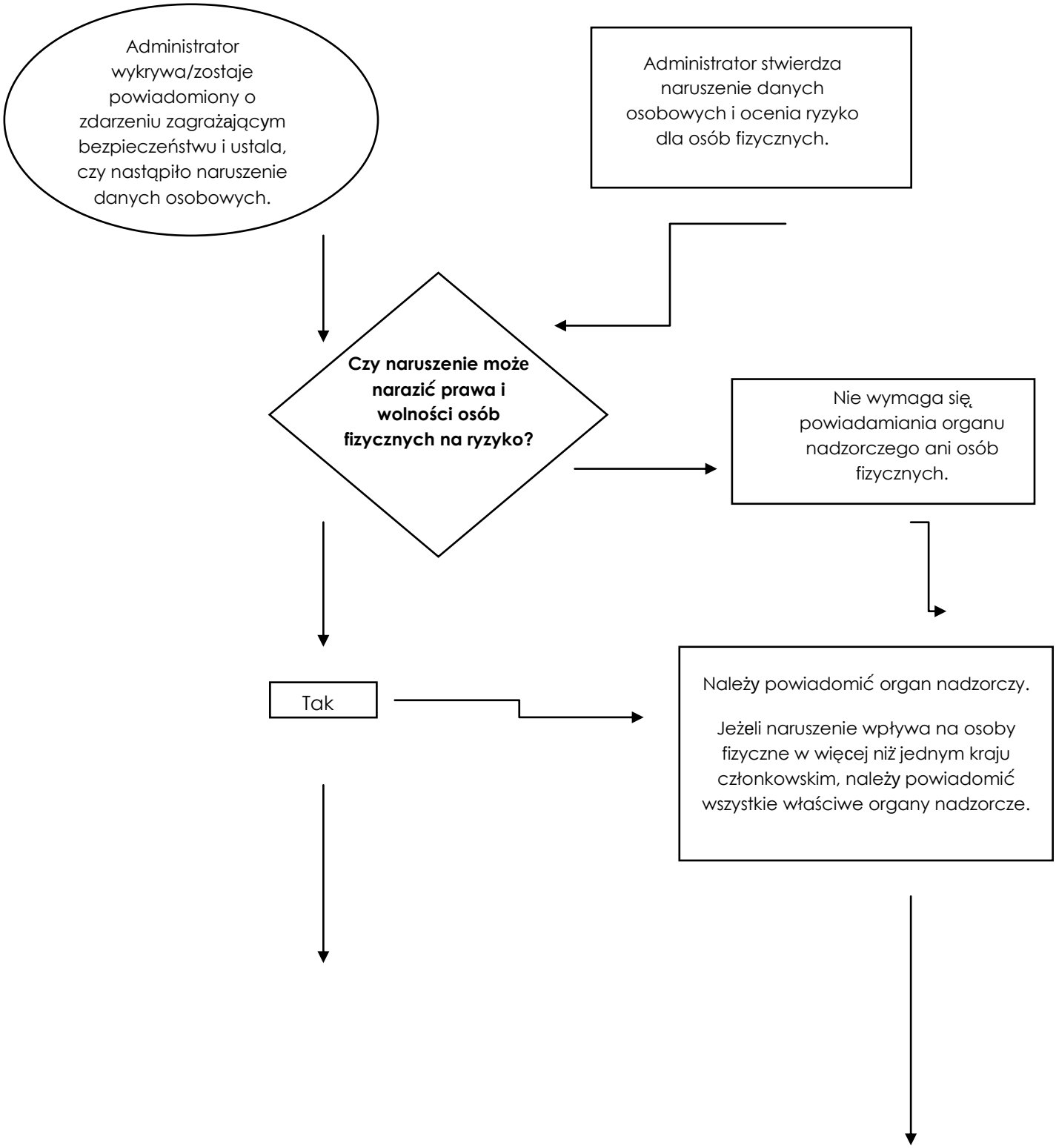
Rejestr naruszeń ochrony danych osobowych					
Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze
1.					
2.					
…					

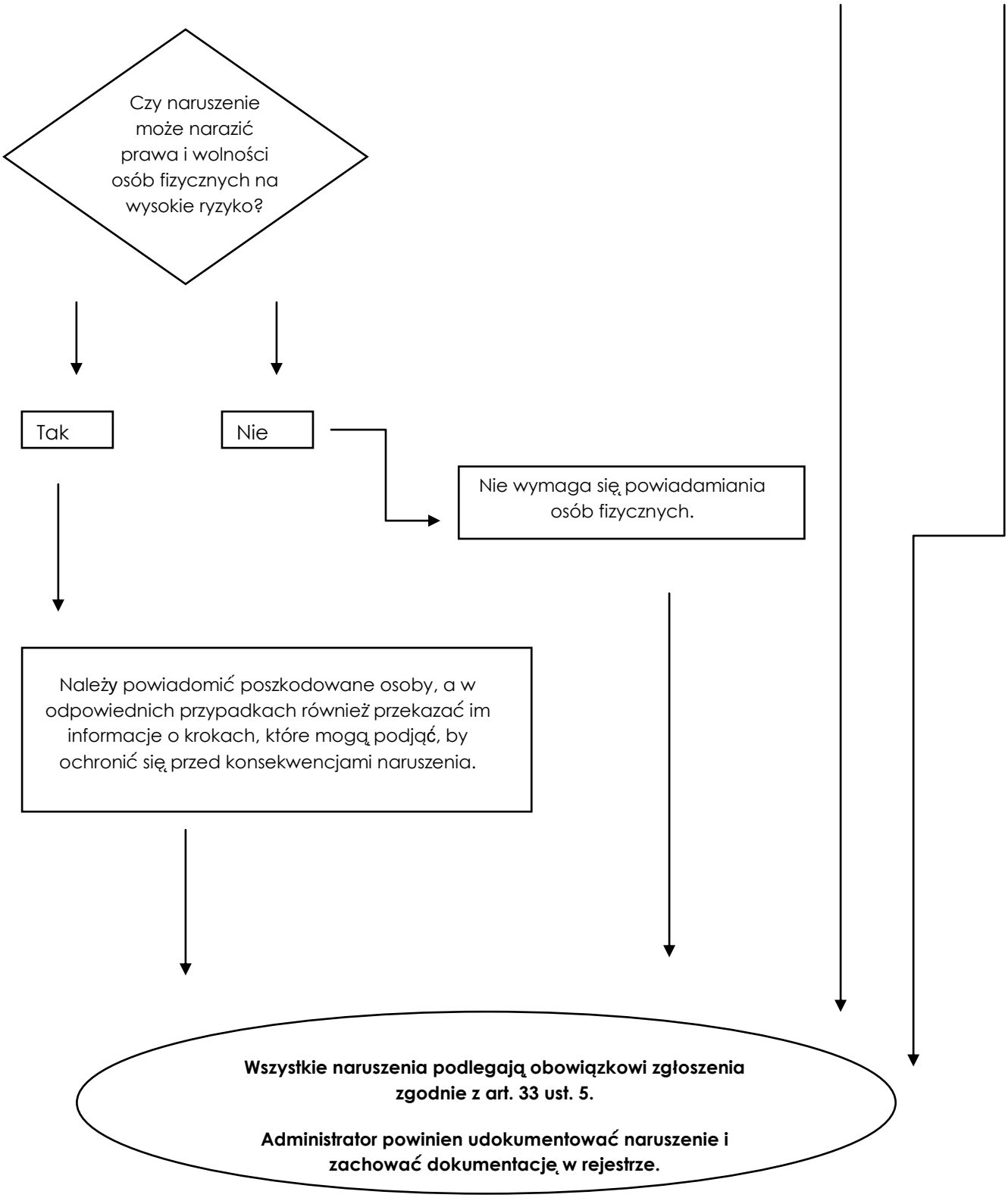
_____

data i podpis Administratora

ZAŁĄCZNIK NR 11

SCHEMAT POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH




Czy naruszenie może narazić prawa i wolności osób fizycznych na wysokie ryzyko?
Tak
Nie
Nie wymaga się powiadamiania osób fizycznych.
Należy powiadomić poszkodowane osoby, a w odpowiednich przypadkach również przekazać im informacje o krokach, które mogą podjąć, by ochronić się przed konsekwencjami naruszenia.
Wszystkie naruszenia podlegają obowiązkowi zgłoszenia zgodnie z art. 33 ust. 5.
Administrator powinien udokumentować naruszenie i zachować dokumentację w rejestrze.