Z A T W I E R D Z A M

…….
Dnia 29 grudnia 2022 r.
Przedsiębiorca: Paulina Leszczyńska

POLITYKA OCHRONY DANYCH OSOBOWYCH
OBOWIĄZUJĄCA W
„MKK PAULINA LESZCZYŃSKA”

Otwock 2022

SPIS TREŚCI

WPROWADZENIE

Niniejszy dokument opisuje reguły oraz procedury dotyczące sposobu oraz bezpieczeństwa przetwarzania Danych Osobowych, w tym z użyciem systemów informatycznych przez Administratora tj. Paulinę Leszczyńską prowadzącą działalność gospodarczą pod firmą *„MKK Paulina Leszczyńska”* z zakładem głównym pod adresem: ul. Bracka 3A, 05-400 Otwock, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP: 5321975558, REGON: 363608803.

Niniejszy dokument ma zastosowanie do przetwarzania wszelkich Danych Osobowych gromadzonych przez Administratora, pobieranych zarówno bezpośrednio od osób, których Dane dotyczą, jak i pośrednio (z innych źródeł), w tym:

a) Danych Osobowych pobieranych przez Administratora:
   - za pośrednictwem strony internetowej www.pleszczynska.com, w tym poprzez formularz kontaktowy,
   - za pośrednictwem poczty elektronicznej, numerów telefonów i poczty tradycyjnej przez – odpowiednio - adresy e-mail, numery telefonów i adresy wskazane na powyższej stronie internetowej,
   - za pośrednictwem social media, takich jak Facebook, Instagram, YouTube, TikTok,
b) Danych Osobowych, które Administrator przetwarza jako Podmiot przetwarzający,
c) Danych Osobowych udostępnionych Administratorowi przez inne podmioty.

Opisane reguły i procedury określają granice dopuszczalnego zachowania wszystkich osób przetwarzających Dane Osobowe zatrudnionych oraz współpracujących z Administratorem, konsekwencje, jakie mogą wystąpić w razie ich naruszenia oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń w związku z naruszeniem bezpieczeństwa przetwarzania Danych Osobowych. Realizacja postanowień tego dokumentu ma zapewnić w szczególności ochronę Danych Osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa przetwarzania, zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa Danych przetwarzanych w systemach informatycznych oraz zagwarantować egzekwowalność uprawnień osób, których Dane dotyczą. Mając to na względzie, niniejsza Polityka Ochrony Danych Osobowych określa przede wszystkim sposób postępowania w przypadku:

a) jakiegokolwiek przetwarzania Danych Osobowych, niezależnie od tego z jakich źródeł Dane te pochodzą, w jakim celu są przetwarzane oraz jakich kategorii Danych Osobowych dotyczy przetwarzanie,
b) stwierdzenia naruszenia bezpieczeństwa ochrony Danych Osobowych,
c) stwierdzenia naruszenia zabezpieczenia systemów informatycznych, w jakich Dane są przetwarzane,
d) zapobiegania skutkom naruszenia bezpieczeństwa przetwarzania Danych Osobowych.

Niniejsza Polityka Ochrony Danych Osobowych obowiązuje wszystkich osób dokonujących jakichkolwiek operacji na Danych Osobowych w firmie Administratora.

Celem niniejszego dokumentu oraz opisanych w nim reguł i procedur jest realizacja następujących postulatów:

a) spełnienie wymagań prawnych dotyczących przetwarzania Danych Osobowych jako cel podstawowy,
b) zwiększenie świadomości co do wagi i wartości informacji wynikających z Danych Osobowych,
c) konieczność ochrony Danych Osobowych oraz dóbr osobistych osób, których Dane dotyczą,
d) ochrona informacji oraz zapewnienie prywatności i godności każdego klienta, kontrahenta oraz wszystkich innych kategorii osób, których Dane dotyczą,

e) ciągłe uczenie się i wyciąganie wniosków z błędów,

f) stałe doskonalenie rozwiązań dostosowujących działania do nowych celów oraz potencjalnych zagrożeń związanych z przetwarzaniem Danych Osobowych,

g) uświadomienie i zapewnienie, że osoby przetwarzające Dane Osobowe są zobowiązane do przestrzegania szczegółowych zasad postępowania wskazanych w niniejszym dokumencie.

ROZDZIAŁ I. PRZEPISY WPROWADZAJĄCE.

1. DEFINICJE

Użyte w niniejszym dokumencie określania oznaczają:

a) **Administrator Danych Osobowych (Administrator)** – Paulina Leszczyńska prowadząca działalność gospodarczą pod firmą *„MKK Paulina Leszczyńska”* z zakładem głównym pod adresem: ul. Bracka 3A, 05-400 Otwock, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP: 5321975558, REGON: 363608803,

b) **Administrator Systemu** – osoba odpowiedzialna za zapewnienie ciągłości i poprawności działania Systemu Informatycznego lub aplikacji, którą może być Administrator lub inna osoba upoważniona przez Administratora,

c) **Dane Osobowe (Dane)** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

d) **Hasło** – ciąg znaków literowych, cyfrowych lub innych pozwalający na dostęp do Systemu Informatycznego, znany jedynie danemu Użytkownikowi,

e) **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący danego Użytkownika,

f) **Integralność** – właściwość zapewniająca, że Dane Osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

g) **Podmiot przetwarzający** – podmiot, o którym mowa w art. 28 RODO, który dokonuje czynności przetwarzania Danych Osobowych na zlecenie Administratora,

h) **Polityka** – niniejsza Polityka Ochrony Danych Osobowych obowiązująca u Administratora,

i) **Poufność** – właściwość zapewniająca, że Dane Osobowe nie są udostępniane nieupoważnionym podmiotom,

j) **Profilowanie** – dowolne zautomatyzowane przetwarzanie Danych Osobowych pozwalające ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której Dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa,

k) **przetwarzanie Danych Osobowych** – jakiekolwiek operacje wykonywane na Danych Osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie i inne, a zwłaszcza te, które wykonuje się w ramach Systemu Informatycznego,

l) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych pełniący funkcję organu nadzorczego na terenie Rzeczpospolitej Polskiej w rozumieniu art. 4 pkt 21 w zw. z art. 51 ust. 1 RODO,

m) **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 (ogólne rozporządzenie o ochronie danych),

n) **Sieć Telekomunikacyjna** – sieć telekomunikacyjna oraz publiczna sieć telekomunikacyjna w rozumieniu odpowiednio art. 2 pkt 29 i 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, w tym w szczególności Internet,

o) **System Informatyczny** – zbiór powiązanych ze sobą elementów, tj. serwerów z systemami operacyjnymi, systemu zarządzania wszelkimi informacjami i danymi (w tym Danymi Osobowymi), oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, terminali, drukarek etc.) oraz urządzeń służących do komunikacji między sprzętowymi elementami Systemu Informatycznego,

p) **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,

q) **Użytkownik (Użytkownicy)** – Administrator, osoba działająca w imieniu Administratora oraz każda inna osoba, która uzyskała od Administratora uprawnienie do bezpośredniego dostępu do Danych Osobowych, w tym w szczególności przetwarzanych w Systemie Informatycznym, posiadająca ustalony indywidualny Identyfikator oraz Hasło.

2. PODSTAWA PRAWNA.

Niniejsza Polityka jest zgodna i sporządzona w oparciu o następujące akty prawne:

a) Konstytucja Rzeczypospolitej Polskiej,
b) 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 (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE. L Nr 119, str. 1, zwane dalej **RODO**,
c) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781),
d) ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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. U. z 2019 r. poz. 730,
e) akty wykonawcze do powyższych aktów prawnych , w zakresie w jakim dotyczą ochrony danych osobowych,
f) inne właściwe przepisy dotyczące ochrony danych osobowych.

ROZDZIAŁ II. PODSTAWOWE ZASADY ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH.

1. ZAKRES OBOWIĄZYWANIA.

1.1. Jeżeli Administrator udzielił pełnomocnictwa w zakresie reprezentowania go we wszelkich sprawach dotyczących ochrony danych osobowych i wynika to z dokumentu pełnomocnictwa, wówczas wszędzie, gdzie jest mowa o Administratorze, należy przez to rozumieć również stosownie umocowanego pełnomocnika Administratora.

1.2. Ochrona Danych Osobowych przetwarzanych przez Administratora obowiązuje wszystkich Użytkowników, tj. osoby, które mają dostęp do Danych Osobowych podlegających przetwarzaniu, bez względu na zajmowane stanowisko, miejsce dokonywania czynności oraz charakter stosunku prawnego łączącego Użytkownika z Administratorem.

1.3. Użytkownicy są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu Danych Osobowych osobom nieupoważnionym, w tym w szczególności procedur i zasad wskazanych w niniejszej Polityce.

1.4. Zachowanie tajemnicy w zakresie Danych Osobowych obowiązuje zarówno podczas trwania stosunku pracy lub innej umowy łączącej Użytkownika z Administratorem, jak również po ustaniu tych stosunków prawnych.

1.5. Administrator jest odpowiedzialny za nadzór nad tworzeniem, wdrażaniem, administracją i interpretacją niniejszej Polityki oraz innych standardów, zaleceń oraz procedur dotyczących ochrony Danych Osobowych.

1.6. Polecenia Administratora, a także innych osób delegowanych i wyznaczonych do działań związanych z ochroną Danych Osobowych oraz z ochroną informacji i bezpieczeństwa Systemu Informatycznego, muszą być bezwzględnie wykonywane przez wszystkich Użytkowników Systemu Informatycznego.

2. ZASADY PRZETWARZANIA ORAZ OCHRONY DANYCH OSOBOWYCH.

2.1. Dane osobowe mogą być:

a) przetwarzane wyłącznie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której Dane dotyczą,

b) zbierane wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami,

c) przetwarzane w sposób adekwatny, stosowny oraz ograniczony do tego, co jest niezbędne do celów, w których są przetwarzane,

d) prawidłowe i w razie potrzeby uaktualniane, w tym w szczególności na wniosek osoby której Dane dotyczą,

e) przechowywane w formie umożliwiającej identyfikację osoby, której Dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których Dane te są przetwarzane,

f) przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, w tym w szczególności za pomocą odpowiednich środków technicznych lub organizacyjnych,

g) przetwarzane wyłącznie w obszarach do tego celu przeznaczonych, przy czym w szczególnych przypadkach możliwe jest przetwarzanie Danych Osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), pod warunkiem uprzedniego poinformowania oraz uzyskania zgody Administratora.

2.2. Dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe, znajdują się serwery lub przechowywane są kopie zapasowe, mogą mieć wyłącznie osoby, które posiadają do tego odpowiednie upoważnienie od Administratora.

2.3. Wszystkich Użytkowników obowiązuje:

a) zasada *„czystego biurka”*, zgodnie z którą zabronione jest pozostawianie jakichkolwiek dokumentów z Danymi Osobowymi podczas nieobecności Użytkownika przy jego stanowisku pracy, zarówno w czasie pracy, jak i po jej zakończeniu, w sposób umożliwiający zapoznanie się innym osobom z Danymi Osobowymi zamieszczonymi na tych dokumentach, chyba że nie ma możliwości, aby inna osoba uzyskała dostęp do takich dokumentów,

b) zasada *„czystego ekranu”*, zgodnie z którą zabronione jest pozostawianie sprzętu służbowego (np. komputera, laptopa, tableta, smartfona) przez Użytkownika bez uprzedniego wylogowania się z Systemu Informatycznego albo zablokowania dostęp do pulpitu stacji roboczej, z której Użytkownik korzysta przy przetwarzaniu Danych Osobowych, a w przypadku zakończenia pracy z Systemem Informatycznym należy zamknąć wszelkie pliki zawierające Dane Osobowe, chyba że nie ma możliwości, aby inna osoba uzyskała dostęp do sprzętu Użytkownika.

Powyższe zasady mają na celu uniemożliwienie osobom nieupoważnionym dostępu do Danych Osobowych przetwarzanych przez Użytkowników.

3. PODSTAWY PRAWNE DO PRZETWARZANIA DANYCH OSOBOWYCH.

3.1. Przetwarzanie Danych Osobowych przez Administratora możliwe jest pod warunkiem, że:

a) osoba, której Dane dotyczą, wyraziła zgodę na przetwarzanie swoich Danych Osobowych w jednym lub większej liczbie określonych celów, w postaci stosownego oświadczenia lub wyraźnego działania potwierdzającego,

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której Dane dotyczą, lub do podjęcia działań na żądanie osoby, której Dane dotyczą, przed zawarciem umowy,

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej,

e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której Dane dotyczą, wymagające ochrony jej Danych Osobowych, w szczególności, gdy osoba, której Dane dotyczą, jest dzieckiem.

3.2. Administrator zobowiązuje się nie przetwarzać Danych Osobowych, jeżeli nie zajdzie jedna z przesłanek, o których mowa w punkcie poprzedzającym.

ROZDZIAŁ III. ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH OSOBOWYCH.

1. PRZETWARZANIE DANYCH OSOBOWYCH.

1.1. Administrator dokonuje przetwarzania Danych Osobowych jako ich Administrator, a także – jeżeli ma to zastosowanie i spełnione zostaną przesłanki wynikające z art. 28 RODO – jako Podmiot przetwarzający.

1.2. Wykaz kategorii osób, których Dane Osobowe są przetwarzane, oraz zakres czynności dotyczących ich przetwarzania, stanowią rejestr czynności przetwarzania Danych Osobowych, stanowiący Załącznik nr 1 do niniejszej Polityki.

1.3. W przypadku istnienia więcej niż jednej kategorii osób, których Dane Osobowe są przetwarzane, każdą z tych kategorii uwzględnia się odrębnie w rejestrze czynności przetwarzania, o którym mowa w punkcie poprzedzającym. W przypadku Administratora wyróżnia się następujące kategorie osób, których Dane Osobowe są przetwarzane: Klienci, Kontrahenci.

1.4. Jeżeli Administrator jest Podmiotem przetwarzającym względem innego administratora, wówczas zobowiązany on jest do prowadzenia rejestru kategorii czynności przetwarzania dokonywanych w imieniu innego administratora, stanowiący Załącznik nr 2 do niniejszej Polityki.

1.5. Rejestry, o których mowa powyżej, są w miarę potrzeby aktualizowane. W przypadku systemów, które są rozbudowywane, wprowadzone zmiany powinny zostać uwzględnione w niniejszej Polityce.

1.6. Szczegóły dotyczące treści oraz prowadzenia rejestrów, o których mowa powyżej, określone zostały w pkt III.5. poniżej.

2. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ.

2.1. W przypadku przekazania do Administratora od osoby, której Dane dotyczą:

a) żądania dostępu do Danych Osobowych - Administrator zobowiązany jest spełnić wobec niej obowiązek informacyjny, a także dostarczyć w formie elektronicznej na adres e-mail wnioskodawcy treść stosowanej klauzuli informacyjnej oraz udzielenia innych informacji żądanych przez wnioskodawcę, a mieszczących się w zakresie tego uprawnienia,

b) żądania przekazania kopii swoich Danych Osobowych - Administrator dostarcza takie kopie w formie elektronicznej na adres e-mail wskazany przez wnioskodawcę, przy czym nie pobiera opłat za kopie Danych w przypadku przekazania

pierwszego egzemplarza kopii, ale w przypadku kolejnych kopii może pobierać opłaty odpowiadające realnym kosztom ich sporządzenia oraz dostarczenia,

c) żądania sprostowania lub uaktualnienia Danych Osobowych - Administrator dokonuje stosownych zmian w swoim Systemie Informatycznym lub w innej stosownej formie, informując jednocześnie o tych czynnościach wnioskodawcę w formie elektronicznej na jego adres e-mail,

d) żądania usunięcia Danych (prawo do bycia zapomnianym) - Administrator usuwa lub anonimizuje Dane Osobowe wnipskdoawcy, pod warunkiem, że nie jest zobowiązany do ich zachowania w związku z przepisami prawa lub spełnieniem spoczywającego na nim obowiązku prawnego,

e) żądania dotyczącego ograniczenia przetwarzania Danych Osobowych w przypadkach przewidzianych w przepisach RODO - Administrator zobowiązany jest do ograniczenia przetwarzania tych Danych Osobowych do niezbędnego minimum, aż do momentu wyjaśnienia sprawy oraz przekazania wnioskodawcy informacji, które uprawdopodobnią prawidłowość przetwarzania oraz umożliwią dalsze przetwarzanie Danych Osobowych przez Administratora,

f) żądania dotyczącego przeniesienia Danych Osobowych do innego administratora Danych Osobowych w przypadkach przewidzianych w przepisach RODO - Administrator zobowiązany jest do przekazania Danych wskazanych przez wnioskodawcę w sposób zapewniający odpowiednie bezpieczeństwo Danych oraz poszanowanie pozostałych praw wynikających z przepisów powszechnie obowiązujących, w powszechnie używanym formacie, o ile jest to technicznie możliwe, a w sytuacji, gdy nie jest to technicznie możliwe, wnioskodawca otrzyma od Administratora dotyczące go Dane Osobowe w powszechnie używanym formacie w celu przesłania ich bezpośrednio innemu administratorowi we własnym zakresie.

2.2. Administrator powinien spełnić żądania osoby, której Dane dotyczą, o których mowa w punkcie poprzedzającym, w terminie miesiąca od dnia ich wniesienia. Gdyby jednak wniesione żądanie było skomplikowane lub Administrator otrzymałby dużą liczbę żądań, co powoduje, że zachowanie terminu, o którym mowa w zdaniu poprzedzającym, nie jest możliwe, Administrator zobowiązany jest spełnić żądanie w terminie nie dłuższym niż trzy miesiące od momentu otrzymania żądania, z tym zastrzeżeniem, że w terminie nie dłuższym niż miesiąc od otrzymania żądania przekaże wnioskodawcy informację o planowanym podjęciu działania, a w terminie nie dłuższym niż dwa miesiące od dnia przekazania ww. informacji spełni żądanie osoby, której Dane dotyczą, z zastrzeżeniem pkt 2.5. poniżej.

2.3. Administrator zobowiązany jest do weryfikacji prawnej możliwości spełnienia żądania. Jeżeli z nałożonego na Administratora obowiązku prawnego albo z uprawnienia przysługującego Administratorowi zgodnie z powszechnie obowiązującymi przepisami prawa, będzie wynikało, że nie może on spełnić żądania osoby, której Dane dotyczą, poinformuje on ją o tym w terminach, o których mowa w punkcie poprzedzającym.

2.4. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której Dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której Dane dotyczą, o powodach niepodjęcia działań, możliwości wniesienia skargi do PUODO oraz skorzystania ze środków ochrony prawnej przed sądem.

2.5. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby, której dane dotyczą, a która wniosła co najmniej jedno z żądań, o których mowa w pkt 2.1. powyżej, wówczas Administrator może zwrócić się do wnioskodawcy w celu potwierdzenia lub udokumentowania jego tożsamości, w tym w szczególności poprzez weryfikację Danych Osobowych i informacji znajdujących się w posiadaniu Administratora.

3. OBOWIĄZEK INFORMACYJNY.

3.1. Każda osoba, której Dane Osobowe będą przetwarzane przez Administratora, ma prawo do bycia informowanym o przetwarzaniu jej Danych Osobowych. W związku z tym, wobec osób, których Dane dotyczą, Administrator zobowiązany jest wypełniać obowiązek informacyjny.

3.2. Obowiązek informacyjny spełniany jest wobec wszystkich osób, których Dane dotyczą, a które to Dane są przez Administratora przetwarzane, niezależnie od celu ich przetwarzania.

3.3. Obowiązek informacyjny Administratora powinien obejmować ujawnienie informacji, takich jak:

a) tożsamość i dane kontaktowe Administratora oraz – gdy ma to zastosowanie – tożsamość i dane kontaktowe przedstawiciela Administratora,

b) cele przetwarzania Danych Osobowych oraz podstawa prawna tego przetwarzania,

c) gdy ma to zastosowanie – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,

d) informacje o odbiorcach Danych Osobowych lub o kategoriach odbiorców, jeżeli istnieją,

e) gdy ma to zastosowanie – informacje o zamiarze przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, jak również o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,

f) okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

g) informacja o prawie do żądania od Administratora przez osobę, której Dane dotyczą, dostępu do jej Danych Osobowych, ich sprostowania, usunięcia (bycia zapomnianym), ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu wobec przetwarzania oraz do złożenia skargi do PUODO,

h) jeżeli ma to uzasadnienie - informacja o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

i) informacja czy podanie Danych Osobowych jest wymogiem ustawowym lub warunkiem zawarcia umowy oraz czy osoba, której Dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania Danych,

j) informacja o zautomatyzowanym podejmowaniu decyzji, w tym o Profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której Dane dotyczą.

3.4. Obowiązek informacyjny Administrator spełnia przez przekazanie klauzuli informacyjnej drogą elektroniczną (na adres e-mail lub poprzez udostępnienie na swojej stronie internetowej) albo w formie papierowej jako załącznik do umów zawieranych z osobami, których Dane dotyczą, lub poprzez zawieszenie i udostępnienie tej informacji w lokalu przedsiębiorstwa.

3.5. Niedopuszczalnym jest niewypełnienie obowiązku informacyjnego przez Administratora.

3.6. Obowiązek informacyjny spełniany jest również wobec osób, których Dane Osobowe zostały Administratorowi udostępnione, tj. pochodzą z innych źródeł niż osoby, których Dane dotyczą. W takim przypadku treść obowiązku informacyjnego dostarczana jest osobie, której Dane dotyczą, po wejściu przez Administratora w posiadanie jej Danych Osobowych lub przy pierwszym kontakcie z taką osobą. Postanowienia pkt 3.1.-3.5. stosuje się odpowiednio, z uwzględnieniem pkt 3.7. poniżej.

3.7. Obowiązek informacyjny Administratora powinien obejmować ujawnienie informacji, takich jak:

a) tożsamość i dane kontaktowe Administratora oraz - gdy ma to zastosowanie - tożsamość i dane kontaktowe jego przedstawiciela,
b) cele przetwarzania, do których mają posłużyć Dane Osobowe, oraz podstawę prawną przetwarzania,
c) kategorie odnośnych Danych Osobowych,
d) informacje o odbiorcach Danych Osobowych lub o kategoriach odbiorców, jeżeli istnieją,
e) gdy ma to zastosowanie – informacje o zamiarze przekazania Danych Osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, jak również o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
f) okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe - kryteria ustalania tego okresu,
g) jeżeli ma to uzasadnienie – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,
h) informacje o prawie do żądania od Administratora dostępu do Danych Osobowych dotyczących osoby, której Dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia Danych,
i) jeżeli ma to uzasadnienie – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
j) informacje o prawie wniesienia skargi do PUODO,
k) informacje o źródle pochodzenia Danych Osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych,
l) informacja o zautomatyzowanym podejmowaniu decyzji, w tym o Profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której Dane dotyczą.

4. ANALIZA RYZYKA I OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH.

4.1. Administrator szacuje prawdopodobieństwo naruszenia bezpieczeństwa przetwarzania Danych Osobowych przede wszystkim poprzez przeprowadzenie analizy ryzyka stanowiącej Załącznik nr 4 do niniejszej Polityki, a w razie, gdy z analizy ryzyka wynika taka konieczność – Administrator przeprowadza ocenę skutków planowanych operacji przetwarzania Danych Osobowych przed wprowadzeniem nowych rozwiązań, które mogą mieć wpływ na to przetwarzanie u Administratora, z uwzględnieniem poniższych postanowień.

4.2. W przypadku konieczności sporządzenia oceny skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, stanowi ona Załącznik nr 5 do niniejszej Polityki.

4.3. W przypadku istnienia więcej niż jednego rodzaju planowanych operacji, dla której należy przeprowadzić ocenę skutków planowanych operacji przetwarzania Danych Osobowych, powinien zostać sporządzony odrębny Załącznik do niniejszej Polityki opatrzony odpowiednio numerem 5a, 5b itd. dla każdego rodzaju ocenianych operacji z osobna.

4.4. Administrator przeprowadza ocenę skutków planowanych operacji przetwarzania Danych Osobowych w przypadku jednoczesnego wystąpienia co najmniej dwóch z poniższych przypadków w ramach działalności Administratora z przetwarzanymi przez niego Danymi Osobowymi:

a) ocena i scoring, w tym Profilowanie i przewidywanie, w szczególności dotyczące takich czynników osobowych osoby, której Dane dotyczą, jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się,

b) zautomatyzowane podejmowanie decyzji, w tym Profilowanie, wywołujące skutki prawne lub wpływające na osobę, której Dane dotyczą, w podobny sposób,

c) systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie osoby, której Dane dotyczą, w tym systematyczne monitorowanie miejsc dostępnych publicznie,

d) przetwarzanie szczególnych kategorii Danych Osobowych z art. 9 ust. 1 (tzw. dane wrażliwe) i art. 10 (dane dotyczące karalności) RODO,

e) przetwarzane Danych Osobowych na dużą skalę,

f) przetwarzanie Danych Osobowych podlegających łączeniu lub dopasowywaniu,

g) wykorzystanie do przetwarzania Danych Osobowych innowacyjnych rozwiązań technicznych lub organizacyjnych, zwłaszcza w kontekście nowatorskich technologii wykorzystujących np. biometrię,

h) transfer danych poza granice Europejskiego Obszaru Gospodarczego,

i) przetwarzanie Danych, które samo w sobie utrudnia osobie, której Dane dotyczą, wykonywanie przysługujących jej praw, korzystanie z usługi czy zawarcie umowy,

j) w sytuacji, gdy z przeprowadzonej analizy ryzyka stanowiącej Załącznik nr 4 do niniejszej Polityki wynika, że prawdopodobne jest wystąpienie zdarzeń, które spowodują wysokie lub bardzo wysokie ryzyko naruszenia ochrony Danych Osobowych.

4.5. Ocena skutków planowanych operacji przetwarzania Danych Osobowych dokonana przez Administratora Danych Osobowych powinna zawierać co najmniej:

a) opis planowanych operacji przetwarzania Danych Osobowych i celów tego przetwarzania,

b) ocenę niezbędności i proporcjonalności przetwarzania w stosunku do celów tj. wskazanie czy określonego - potencjalnie ryzykownego - działania można uniknąć lub, jeśli nie ma takiej możliwości, jakie środki zastosowano, aby ryzyko zostało zminimalizowane,

c) ocenę ryzyka naruszenia praw i wolności osoby, której Dane dotyczą, w szczególności, aby Administrator zdawał sobie sprawę z ryzyka, jakie niesie wykorzystywana technologia,

d) środki planowane w celu zaradzenia ryzyku oraz wykazania zgodności operacji przetwarzania Danych Osobowych z obowiązującymi przepisami prawa.

5. REJESTR CZYNNOŚCI PRZETWARZANIA / REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA.

5.1. Administrator prowadzi rejestr czynności przetwarzania Danych Osobowych dla poszczególnych kategorii osób, których Dane Osobowe są przetwarzane, stanowiący Załącznik nr 1 do niniejszej Polityki.

5.2. Jeżeli Administrator jest względem innego administratora Podmiotem przetwarzającym Dane Osobowe w rozumieniu art. 28 RODO, wówczas zobowiązany jest prowadzić rejestr kategorii czynności przetwarzania dokonywanych w imieniu innego administratora stanowiący Załącznik nr 2 do niniejszej Polityki.

5.3. Rejestr czynności przetwarzania Danych Osobowych zawiera informację dotyczące:

a) danych identyfikujących Administratora, w tym jego nazwy oraz danych kontaktowych,

b) celów, w jakich są przetwarzane Dane Osobowe,
c) opisu kategorii osób, których Dane dotyczą, oraz kategorii Danych Osobowych,
d) kategorii odbiorców, którym Dane zostały lub zostaną ujawnione,
e) odnotowanie faktu przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej,
f) planowane terminy usunięcia poszczególnych kategorii Danych Osobowych,
g) ogólnego opisu technicznego i organizacyjnego środków bezpieczeństwa.

5.4. Rejestr kategorii czynności przetwarzania dokonywanych w imieniu innego administratora zawiera informacje dotyczące:
a) danych identyfikujących Podmiot przetwarzający oraz administratora, w imieniu którego działa Podmiot przetwarzający,
b) kategorii przetwarzań dokonywanych w imieniu administratora wynikających z celu świadczonych usług lub zawartej umowy powierzenia,
c) odnotowania faktu przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej,
d) ogólnego opisu technicznego i organizacyjnego środków bezpieczeństwa.

6. INNE CZYNNOŚCI ZWIĄZANE Z BEZPIECZEŃSTWEM DANYCH OSOBOWYCH.

6.1. Administrator zobowiązany jest do współpracy z PUODO, która może dotyczyć w szczególności zgłaszania naruszeń, a także uprzednich konsultacji dotyczących właściwego przetwarzania Danych Osobowych.

6.2. W przypadku wystąpienia naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, Administrator zobowiązany jest do zawiadomienia PUODO w terminie 72 godzin od momentu stwierdzeniu naruszenia.

6.3. Zgłoszenie naruszenia powinno zawierać co najmniej:
a) opis charakteru naruszenia ochrony Danych Osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których Dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów Danych Osobowych, których dotyczy naruszenie,
b) zawierać oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji na temat naruszenia,
c) opisywać możliwe konsekwencje naruszenia ochrony Danych Osobowych,
d) opisywać środki zastosowane lub proponowane przez Administratora Danych Osobowych w celu zaradzenia na przyszłość naruszaniu ochrony Danych Osobowych, w tym w stosownych przypadkach – planowane środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6.4. Administrator zobowiązany jest – z wyjątkiem przypadków przewidzianych w przepisach RODO - zawiadomić bez zbędnej zwłoki osobę, której Dane dotyczą, o każdym przypadku naruszenia ochrony Danych Osobowych jej dotyczących, szczególnie jeżeli incydent ten może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

6.5. Zawiadomienie osoby, której Dane dotyczą, musi zawierać co najmniej:
a) oznaczenie punktu kontaktowego, który pozwoli uzyskać więcej informacji,
b) opisywać możliwe konsekwencje naruszenia ochrony Danych Osobowych,

c) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszaniu ochrony Danych Osobowych, w tym w stosownych przypadkach – środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6.6. Zawiadomienie, o którym mowa w punkcie poprzedzającym, nie jest konieczne jeżeli:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne oraz środki ochrony (w tym w szczególności takie jak pseudonimizacja Danych Osobowych, o której mowa w pkt 6.7. lit. a poniżej) i środki te zostały zastosowane do Danych Osobowych, których dotyczy naruszenie, a stosowanie tych środków powoduje, że nawet naruszenie ochrony Danych nie spowoduje powstania dodatkowego obowiązku informacyjnego (zawiadomienia),

b) w dalszej kolejności Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której Dane dotyczą,

c) wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których Dane dotyczą, zostają poinformowane w równie skuteczny sposób.

6.7. Administrator w celu zabezpieczenia przetwarzanych Danych Osobowych - w miarę możliwości - stosuje technikę:

a) pseudonimizacji Danych Osobowych, polegającą na odwracalnym procesie, po którego przeprowadzeniu w przyszłości nie będzie możliwe zidentyfikowanie określonej osoby bez użycia dodatkowych informacji, pod warunkiem osobnego przechowywania tych dodatkowych informacji oraz zabezpieczenia ich odpowiednimi środkami technicznymi i organizacyjnymi uniemożliwiającymi przypisanie Danych konkretnej osobie,

b) anonimizacji Danych Osobowych, polegającą na nieodwracalnym procesie, po którego przeprowadzeniu w przyszłości nie będzie możliwe zidentyfikowanie określonej osoby na podstawie posiadanych przez Administratora informacji.

ROZDZIAŁ IV. TRANSFER DANYCH OSOBOWYCH.

1. POWIERZENIE DO PRZETWARZANIA DANYCH OSOBOWYCH.

1.1. Administrator może powierzać Dane Osobowe Podmiotom przetwarzającym, które będą przetwarzać te Dane wyłącznie na polecenie i w imieniu Administratora. W takim przypadku, przetwarzanie Danych Osobowych odbywa się wyłącznie na podstawie umowy powierzenia przetwarzania Danych Osobowych zawartej pomiędzy Administratorem a Podmiotem przetwarzającym, zwaną dalej **Umową powierzenia**.

1.2. Umowa powierzenia może być zawarta w formie pisemnej lub dokumentowej i powinna zawierać ściśle określony zakres powierzonych do przetwarzania Danych.

1.3. Przetwarzanie Danych Osobowych możliwe jest tylko w zakresie ustalonym przez Umowę powierzenia.

1.4. Powierzone Dane podlegają przetwarzaniu i ochronie na co najmniej takich samych zasadach, jakie stosuje Administrator, chyba że Umowa powierzenia określi inne zasady ochrony powierzonych Danych Osobowych, pod warunkiem, że będą one zgodne z RODO i będą zwiększać poziom bezpieczeństwa tych Danych.

1.5. Zmiana zasad związanych z ochroną powierzonych Danych Osobowych oraz ich przetwarzaniem przez Podmiot przetwarzający nie może:

a) naruszać praw osób, których Dane Osobowe zostały powierzone do przetwarzania,

b) naruszać zasad związanych z ochroną Danych Osobowych przewidzianych w przepisach prawa,

c) zmieniać celu przetwarzania powierzonych Danych Osobowych,

d) przetwarzać powierzonych Danych Osobowych w sposób inny niż określony przez Administratora,

e) udostępniać powierzonych Danych Osobowych osobom lub podmiotom trzecim bez zgody Administratora.

1.6. Podmiot przetwarzający zapewnia, że osoby upoważnione przez niego do przetwarzania Danych Osobowych Administratora zobowiązały się do zachowania tajemnicy w związku z przetwarzaniem powierzonych Danych Osobowych.

1.7. Podmiot przetwarzający:

a) zobowiązany jest zapewniać wszelkie środki wymagane do zapewnienia bezpieczeństwa przetwarzania Danych Osobowych,

b) w przypadku korzystania z podwykonawców przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (w takim przypadku mamy do czynienia z tzw. podpowierzeniem przetwarzania Danych Osobowych),

c) pomaga Administratorowi Danych Osobowych poprzez odpowiednie środki techniczne i organizacyjne wywiązywać się z obowiązku odpowiadania na żądania osób, których Dane dotyczą,

d) 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 przepisy prawa nakazują Podmiotowi przetwarzającemu dalsze przechowywanie tych Danych,

e) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków wynikających z powszechnie obowiązujących przepisów prawa, w tym w szczególności z RODO.

2. UDOSTĘPNIANIE DANYCH OSOBOWYCH.

2.1. Administrator nie udostępnia przetwarzanych przez siebie Danych Osobowych innym podmiotom, które stałyby się ich administratorami, chyba że uzyska on zgodę osoby, której Dane dotyczą, lub możliwość udostępnienia Danych Osobowych będzie wynikała z decyzji sądu, organu administracji publicznej lub z innych okoliczności mających umocowanie w przepisach prawa.

2.2. W przypadku udostępniania Danych Osobowych - poza odebraniem stosownych zgód od osób, których Dane dotyczą - Administrator może zawrzeć stosowną umowę dotyczącą udostępniania Danych innym administratorom.

2.3. W przypadku udostępniania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, Administrator Danych Osobowych zastosuje się do wymagań wynikających z przepisów prawa, jak również zgodnie z postanowieniami pkt 3 niniejszego rozdziału.

3. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTWA TRZECIEGO LUB ORGANIZACJI MIĘDZYNARODOWEJ.

3.1. Przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium, określony sektor/sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

3.2. Przekazanie Danych Osobowych, o którym mowa w punkcie poprzedzającym, może nastąpić wyłącznie, gdy Administrator oraz podmiot, któremu Dane przekazano, zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że

zapewnione zostaną egzekwowalne prawa osób, których Dane dotyczą, oraz skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia można zapewnić – bez konieczności uzyskania specjalnego zezwolenia ze strony PUODO – za pomocą:

a) wiążących reguł korporacyjnych zgodnie z art. 47 RODO,
b) standardowych klauzul ochrony Danych przyjętych przez Komisję Europejską zgodnie z procedurą sprawdzającą,
c) standardowych klauzul ochrony Danych przyjętych przez PUODO i zatwierdzonych przez Komisję Europejską zgodnie z procedurą sprawdzającą,
d) zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami Administratora w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których Dane dotyczą,
e) zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami Administratora w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których Dane dotyczą.

3.3. Jeżeli nie zostaną spełnione przesłanki, o których mowa w dwóch punktach poprzedzających, przekazywanie Danych Osobowych do państwa trzeciego może nastąpić pod warunkiem, że:

a) osoba, której Dane dotyczą, została poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,
b) przekazanie jest niezbędne do wykonania umowy między osobą, której Dane dotyczą, a Administratorem, lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której Dane dotyczą,
c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której Dane dotyczą, między Administratorem a inną osobą fizyczną lub prawną,
d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innych osób, jeżeli osoba, której Dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
g) przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes, ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

ROZDZIAŁ V. ZABEZPIECZENIE DANYCH OSOBOWYCH, W TYM RAMACH SYSTEMU INFORMATYCZNEGO.

1. ŚRODKI FIZYCZNE.

1.1. Administrator zobowiązany jest do zastosowania środków technicznych i organizacyjnych zapewniających optymalną ochronę przetwarzanych Danych Osobowych w Systemie Informatycznym, w tym w szczególności zapewniających:

a) zabezpieczenie Danych przed ich udostępnieniem osobom nieupoważnionym,
b) zapobieganie przed pobraniem Danych przez osobę nieuprawnioną,

c) zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu Danych,

d) zapewnianie przetwarzania Danych zgodnie z obowiązującymi przepisami prawa.

1.2. Zadania określone w punkcie poprzedzającym wykonuje lub nadzoruje ich wykonanie Administrator Systemu w imieniu Administratora.

1.3. Zabezpieczenia pomieszczeń, w których przetwarzane są Dane Osobowe, są następujące:

a) samodzielny dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe, ma wyłącznie Administrator, a inne osoby mogą przebywać w takich pomieszczeniach wyłącznie w towarzystwie Administratora lub po uzyskaniu od niego odpowiedniego upoważnienia,

b) pomieszczenia, w których przetwarza się Dane Osobowe, zamykane są na klucze, do których dostęp ma wyłącznie Administrator lub osoby przez niego upoważnione,

c) poza przestrzeganiem zasady *„czystego biurka”* i zasady *„czystego ekranu”*, o których mowa w pkt II.2.4. powyżej – dodatkowo w przypadku opuszczenia pomieszczenia przez Użytkownika, w tym także w godzinach pracy, Dane Osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych,

d) nieaktualne lub błędne wydruki zawierające Dane Osobowe niszczone są w sposób uniemożliwiający odczyt danych np. w niszczarkach,

e) budynek oraz pomieszczenia służące do przetwarzania Danych Osobowych posiadają następujące zabezpieczenia:
- przy ul. Brackiej 3A w Otwocku - brama wjazdowa, drzwi do budynku i pomieszczeń zamykane na klucz,
- przy ul. Ordona 7B/101 w Warszawie - wejście na kod, monitoring wizyjny (należący do zarządcy budynku), brama wjazdowa ze szlabanem, czujka przeciwpożarowa, drzwi do budynku i pomieszczeń zamykane na klucz.

2. ŚRODKI TECHNICZNE.

2.1. Zabezpieczenia przed nieautoryzowanym dostępem do Systemu Informatycznego oraz do Danych Osobowych w nim zamieszczonych, następuje poprzez:

a) podłączenie urządzenia końcowego (komputera, terminala, drukarki) do Sieci Telekomunikacyjnej dokonywane jest przez Administratora, Administratora Systemu lub inną osobę upoważnioną przez Administratora,

b) identyfikację każdego Użytkownika w Systemie Informatycznym w postaci uwierzytelnienia, tj. działania, którego celem jest weryfikacja deklarowanej tożsamości osoby korzystającej z Systemu Informatycznego,

c) przydzielenie każdemu Użytkownikowi indywidualnego Identyfikatora do korzystania z Systemu Informatycznego,

d) stosowanie programu antywirusowego z zaporą antywłamaniową na wszystkich urządzeniach, na których dochodzi do przetwarzania Danych Osobowych,

e) zabezpieczenie Hasłami kont na urządzeniach wskazanych w literze poprzedzającej, z uwzględnieniem minimalnych wymogów Haseł, o których mowa w pkt V.5.8. poniżej,

f) ustawienie monitorów stanowisk przetwarzania Danych Osobowych w sposób uniemożliwiający wgląd w Dane osobom nieuprawnionym.

2.2. Zabezpieczenia przed nieautoryzowanym dostępem do Danych Osobowych poprzez Sieć Telekomunikacyjną:

a) logiczne oddzielenie sieci lokalnej uniemożliwiające uzyskanie dostępu do Danych Osobowych spoza Systemu Informatycznego, jak również uzyskanie dostępu z Systemu Informatycznego do Sieci Telekomunikacyjnej publicznej,

b) zastosowanie zabezpieczenia Sieci Telekomunikacyjnej lokalnej w postaci lokalnej bramy sieciowej z zainstalowanym systemem typu firewall.

2.3. Zabezpieczenia przed utratą Danych Osobowych w wyniku awarii:

a) ochrona sprzętu komputerowego przed zanikiem zasilania poprzez stosowanie listw przepięciowych,

b) ochrona przed utratą zgromadzonych Danych Osobowych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są Dane i system operacyjny (tzw. backupy),

c) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego,

d) współpraca z profesjonalnym dostawcą usług hostingowych, u którego Administrator korzysta z przestrzeni serwera.

3. PROCEDURY NADAWANIA I ZMIANY UPRAWNIEŃ DO PRZETWARZANIA DANYCH.

3.1. Każdy Użytkownik Systemu Informatycznego przed przystąpieniem do przetwarzania Danych Osobowych musi zapoznać się z niniejszą Polityką oraz zobowiązuje się ją bezwzględnie stosować.

3.2. Administrator lub osoba przez niego upoważniona przyznaje uprawnienia w zakresie dostępu do Systemu Informatycznego określając zakres uprawnień Użytkownika.

3.3. Administrator, osoba przez niego upoważniona lub Administrator Systemu zakładają konto Użytkownika w Systemie Informatycznym o odpowiednim indywidualnym Identyfikatorze i zabezpieczone indywidualnym Hasłem.

3.4. Hasło uprawniające do korzystania z Systemu Informatycznego Użytkownik wpisuje osobiście.

3.5. Konto zostaje zablokowane lub usunięte przez Administratora, osobę przez niego upoważnioną lub przez Administratora Systemu.

3.6. Hasła dostępu Użytkownika do Systemu Informatycznego stanowią tajemnice służbową znaną wyłącznie temu Użytkownikowi.

3.7. Hasła, w stosunku do których zaistniało podejrzenie o ich ujawnieniu osobie nieuprawnionej, podlegają niezwłocznej zmianie.

3.8. W celu zabezpieczenia awaryjnego dostępu do Systemu Informatycznego, Administrator znajduje się w posiadaniu aktualnego Hasła Administratora Systemu.

3.9. Pełne prawa Administratora Systemu posiada tylko Administrator lub osoba przez niego upoważniona.

3.10. Podczas nieobecności w firmie osoby upoważnionej do wykonywania obowiązków Administratora Systemu (jeżeli nie jest nim Administrator), jego obowiązki wykonuje Administrator lub inna osoba przez niego upoważniona.

4. REJESTROWANIE I USUWANIE UŻYTKOWNIKÓW Z EWIDENCJI SYSTEMU INFORMATYCZNEGO.

4.1. Administrator Systemu prowadzi w imieniu Administratora ewidencję osób dopuszczonych do przetwarzania Danych Osobowych w oparciu o wnioski Administratora o przyznanie lub modyfikację uprawnień.

4.2. W przypadku otrzymania przez Administratora Systemu lub inną osobę upoważnioną przez Administratora, wniosku o zablokowanie lub usunięcie konta Użytkownika w Systemie Informatycznym, osoba ta jest zobowiązana powiadomić o tym Administratora (chyba że wniosek taki wpłynął bezpośrednio do Administratora).

4.3. Usunięcie konta z Systemu Informatycznego następuje na wniosek Administratora lub jest dokonywane przez niego bezpośrednio.

4.4. Konto Użytkownika usuwa Administrator Systemu zgodnie ze szczegółowymi instrukcjami operacyjnymi specyficznymi dla danego Systemu Informatycznego.

5. ZASADY POSŁUGIWANIA SIĘ HASŁAMI.

5.1. Bezpośredni dostęp do Systemu Informatycznego może mieć miejsce wyłącznie po podaniu Identyfikatora Użytkownika i właściwego Hasła.

5.2. Za regularną zmianę Haseł Użytkownika w Systemie Informatycznym odpowiada Użytkownik. Zalecana jest zmiana Hasła nie rzadziej niż co 3 miesiące.

5.3. Hasło Użytkownika powinno być zmienione przed upływem okresu, o którym mowa w punkcie poprzedzającym, jeżeli istnieje podejrzenie, iż jest ono znane osobom nieuprawnionym.

5.4. Identyfikator Użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu Użytkownika z Systemu Informatycznego nie może on zostać przydzielony innej osobie.

5.5. Użytkownicy są odpowiedzialni za zachowanie Poufności swoich Identyfikatorów i Haseł.

5.6. Hasła Użytkowników utrzymuje się w tajemnicy również po upływie ich ważności oraz po ustaniu stosunku pracy.

5.7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że osoba nieupoważniona poznała Hasło w sposób nieuprawniony, Użytkownik zobowiązany jest do poinformowania o zaistniałej sytuacji Administratora Systemu oraz do zmiany Hasła zgodnie z pkt 5.3. powyżej.

5.8. Przy tworzeniu Hasła obowiązują następujące zasady:

a) minimalna długość Hasła to 8 znaków,

b) zakazuje się stosowania:

- Haseł, które Użytkownik stosował uprzednio,
- swojego Identyfikatora w jakiejkolwiek formie,
- swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny),
- ogólnie dostępnych informacji o Użytkowniku (numer telefonu, numer rejestracyjny samochodu itp.),

c) należy stosować Hasła zawierające co najmniej jedną małą literę, jedną dużą literę, jedną cyfrę arabską i jeden znak specjalny,

d) zmiany Hasła nie wolno zlecać innym osobom.

6. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM.

6.1. Rozpoczęcie pracy w Systemie Informatycznym na komputerach Użytkowników wymaga zalogowania przy użyciu indywidualnego Identyfikatora oraz Hasła.

6.2. Przed opuszczeniem stanowiska pracy (w tym także w czasie pracy) należy zablokować stację roboczą lub wylogować się z oprogramowania i Systemu Informatycznego (zasada *„czystego ekranu”*, o której mowa w pkt II.2.4. lit. b powyżej).

6.3. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów oraz wylogować się z Systemu Informatycznego.

6.4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania.

7. PROCEDURY TWORZENIA KOPII ZAPASOWYCH.

7.1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu pod nadzorem Administratora.

7.2. Kopie bezpieczeństwa wykonywane są przez administrację serwera, na którym gromadzone są Dane Osobowe, jeżeli do gromadzenia Danych dochodzi na danym serwerze.

7.3. W przypadku konieczności przechowywania wydruków zawierających Dane Osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom nieuprawnionym. Wydruki, które zawierają Dane Osobowe i są przeznaczone do usunięcia, ulegają zniszczeniu w stopniu uniemożliwiającym ich odczytanie, przede wszystkim poprzez używanie niszczarek.

8. TECHNICZNE ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO.

8.1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspyware.

8.2. Każdy e-mail wpływający na konta pocztowe musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.

8.3. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.

8.4. Bezwzględnie zabrania się pobierania z Sieci Telekomunikacyjnej plików niewiadomego pochodzenia.

8.5. Administrator Systemu przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach, na których przetwarzane są Dane Osobowe, w tym co najmniej raz na jeden miesiąc.

8.6. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto, oraz wszystkie posiadane przez Użytkownika nośniki.

9. ZASADY I SPOSÓB ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH.

9.1. Dane Osobowe przetwarzane z użyciem Systemów Informatycznych mogą być dostępne wyłącznie dla osób uprawnionych wpisanych do ewidencji osób dopuszczonych do przetwarzania Danych Osobowych w Systemie Informatycznym, którą prowadzi Administrator Systemu.

9.2. Udostępnianie Danych Osobowych, o którym mowa w punkcie poprzedzającym, nie może być realizowane drogą telefoniczną.

9.3. System Informatyczny oraz aplikacje wykorzystywane do obsługi Danych Osobowych zapewniają odnotowanie informacji o przekazanych odbiorcom Danych i informacji. Zakres informacji powinien obejmować co najmniej dane odbiorcy, datę przekazania oraz zakres udostępnionych Danych.

10. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO.

10.1. Przeglądy i konserwacja urządzeń:

a) przeglądy i konserwacja urządzeń, programów i narzędzi wchodzących w skład Systemu Informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu lub oprogramowania,

b) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, ich przyczyny przeanalizowane, a o fakcie ujawnienia nieprawidłowości Administrator Systemu jest obowiązany zawiadomić Administratora.

10.2. W przypadku przekazania do naprawy nośników informatycznych zawierających Dane Osobowe lub sprzętu komputerowego, którego nośniki mogą zawierać Dane Osobowe, należy wcześniej wskazać sposób usuwania (tj. zniszczenia, usunięcia Danych Osobowych lub taką ich modyfikację (w tym – w miarę możliwości - pseudonimizację), która nie pozwoli na ustalenie tożsamości osoby, której Dane dotyczą) Danych Osobowych z tych nośników.

11. POŁĄCZENIE Z SIECIĄ TELEKOMUNIKACYJNĄ.

11.1. Połączenie z Siecią Telekomunikacyjną realizowane jest poprzez sieć bezprzewodową z zastosowaniem następujących zasad ochrony:

a) dostęp do Sieci Telekomunikacyjnej wymaga podania klucza składającego się z liter i cyfr oraz zezwolenia na zalogowanie się do Sieci przez Administratora Systemu,

b) każdy komputer posiadający dostęp do Sieci Telekomunikacyjnej posiada oprogramowanie antywirusowe chroniące przed złośliwym oprogramowaniem (antyspyware) oraz zaporę sieciową (firewall),

c) osobie korzystającej z Sieci Telekomunikacyjnej zabrania się wchodzenia na strony niezgodne z prawem lub posiadające wirusy i programy szpiegujące (jak np. trojan, spyware).

11.2. Połączenie z Siecią Telekomunikacyjną publiczną zabezpieczone jest przez moduł firewall działający na routerze sieciowym.

11.3. Na każdym routerze w Systemie Informatycznym działa osobny firewall.

11.4. Zabronione jest połączenie z Siecią Telekomunikacyjną urządzenia służbowego z niedziałającym programem antywirusowym lub firewallem albo ich brakiem.

12. KORZYSTANIE Z KOMPUTERÓW I URZĄDZEŃ PRZENOŚNYCH.

12.1. Administrator dopuszcza korzystanie z komputerów i urządzeń przenośnych, w tym laptopów, tabletów oraz smartfonów.

12.2. Komputery przenośne (laptopy), używane do przetwarzania Danych Osobowych, zabezpieczone są podczas transportu oraz przechowywania przed dostępem do tych Danych osób nieuprawnionych, w szczególności:

a) dostęp do komputerów przenośnych zabezpieczony jest przez Identyfikator i Hasło,

b) nie zezwala się na używanie komputera przenośnego osobom nieupoważnionym do dostępu do Danych Osobowych,

c) zaleca się, aby pliki z Danymi Osobowymi dostępne na komputerze przenośnym były zaszyfrowane.

12.3. Postanowienia punktu poprzedzającego stosuje się odpowiednio do urządzeń przenośnych, w tym tabletów i smartfonów, o których mowa w pkt 12.1. powyżej, przy czym zasady o których mowa w pkt V.5.8. mają zastosowanie w zakresie możliwości technicznych urządzenia przenośnego.

ROZDZIAŁ VI. KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH.

1. Administrator sprawuje nadzór nad przestrzeganiem zasad ochrony Danych Osobowych wynikający z przepisów powszechnie obowiązujących, w tym w szczególności z RODO, oraz zasad ustanowionych w niniejszej Polityce.
2. Administrator może przeprowadzać kontrole oraz dokonywać okresowych audytów bezpieczeństwa przetwarzania Danych Osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w punkcie poprzedzającym, Administrator może sporządzać roczne sprawozdania.
4. Czynności, o których mowa w niniejszym rozdziale, może dokonywać audytor zewnętrzny, który przygotuje odpowiednie sprawozdanie z kontroli w celu przedstawienia go Administratorowi.

ROZDZIAŁ VII. NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

1. MOŻLIWE ZAGROŻENIA DOTYCZĄCE NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

1.1. Podział zagrożeń:

a) **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty Integralności Danych, ich zniszczenia oraz do uszkodzenia infrastruktury technicznej Systemu Informatycznego, a zatem ciągłość Systemu Informatycznego może zostać zakłócona, przy czym w przypadku takich zagrożeń nie dochodzi do naruszenia Poufności Danych,

b) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, Administratora, Podmiotu przetwarzającego, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - ich występowanie może prowadzić do zniszczenia Danych, zakłócenia ciągłości pracy Systemu Informatycznego oraz do naruszenia Poufności Danych np. niezamierzone pomyłki operatorów, Administratora, Podmiotu przetwarzającego, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania,

c) **zagrożenia zamierzone** – świadome i celowe działania powodujące naruszenie Poufności Danych, zazwyczaj nie skutkujące uszkodzeniem infrastruktury technicznej i zakłóceniem ciągłości pracy, zagrożenia te można podzielić na:
   - nieuprawniony dostęp do Systemu Informatycznego z zewnątrz (włamanie do Systemu),
   - nieuprawniony dostęp do Systemu Informatycznego z jego wnętrza,
   - nieuprawnione przekazanie Danych,
   - bezpośrednie zagrożenie materialnych składników Systemu Informatycznego (np. kradzież sprzętu).

1.2. Naruszenie lub podejrzenie naruszenia Systemu informatycznego, w którym przetwarzane są Dane Osobowe, następuje w sytuacji:

a) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby Systemu Informatycznego, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne itp.,

b) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

c) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony Danych,

d) pojawienia się odpowiedniego komunikatu alarmowego,

e) podejrzenia nieuprawnionej modyfikacji Danych w Systemie Informatycznym lub innego odstępstwa od stanu oczekiwanego,

f) naruszenia lub próby naruszenia Integralności Systemu Informatycznego,

g) pracy w Systemie Informatycznym wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony Danych Osobowych, jak np. praca osoby, która nie jest formalnie dopuszczona do użytkowania Systemu Informatycznego,

h) ujawnienia nieautoryzowanych kont dostępu do Systemu Informatycznego,

i) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, jak np. nieprzestrzeganie zasady *„czystego ekranu”*, o której mowa w pkt II.2.4. lit. b powyżej.

1.3. Za naruszenie ochrony Danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania Danych Osobowych, jak np.:

a) niezabezpieczone pomieszczenia,

b) niezabezpieczone urządzenia archiwizujące,

c) pozostawianie Danych w nieodpowiednich miejscach (np. w koszach na śmieci czy w miejscach publicznie dostępnych),

d) pozostawienie niezabezpieczonych dokumentów zawierających Dane Osobowe na stanowisku pracy w razie jego opuszczenia przez osobę przetwarzającą Dane w imieniu Administratora, jak np. nieprzestrzeganie zasady *„czystego biurka”*, o której mowa w pkt II.2.4. lit. a powyżej, pozostawienie dokumentów z Danymi Osobowymi w drukarce.

2. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

2.1. W przypadku stwierdzenia naruszenia:

a) zabezpieczenia Systemu Informatycznego,

b) technicznego stanu urządzeń,

c) zakresu posiadanych Danych Osobowych,

d) jakości transmisji danych w Sieci Telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń,

e) innych zdarzeń mogących mieć wpływ na naruszenie ochrony Danych Osobowych oraz zagrożeń wskazanych w pkt VII.1.1. powyżej,

każda osoba zatrudniona lub współpracująca z Administratorem zobowiązana jest do niezwłocznego powiadomienia o tym fakcie Administratora i swojego bezpośredniego przełożonego.

2.2. Po wykryciu zdarzeń określonych w punkcie poprzedzającym należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia (o ile istnieje taka możliwość), a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców zaistniałej sytuacji,

b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

c) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

d) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji Systemu Informatycznego, aplikacji użytkowej lub innym właściwym dokumencie,

e) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,

f) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora lub innej osoby przez niego upoważnionej.

2.3. Po przybyciu na miejsce naruszenia lub po ujawnieniu naruszenia ochrony Danych Osobowych, Administrator lub osoba przez niego upoważniona:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,

b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

c) jeżeli zachodzi taka potrzeba - zleca usuniecie występujących naruszeń.

2.3 W razie stwierdzonego naruszenia Administrator dokona zgłoszenia naruszenia do PUODO oraz – gdy wymagają tego przepisy RODO – zawiadomienia osób, których Danych Osobowych dotyczyło naruszenie (pkt III.6.2.-6.5. powyżej).

2.4 Administrator lub osoba przez niego upoważniona dokumentuje zaistniały przypadek naruszenia sporządzając stosową notatkę w oparciu o przeprowadzone bezpośrednio czynności lub w oparciu o uzyskane informacje. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez Administratora.

2.5 Analiza, o której mowa w punkcie poprzedzającym, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie osób odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

2.7. Wobec osoby, która w przypadku naruszenia zabezpieczeń Systemu Informatycznego lub uzasadnionego domniemania takiego naruszenia, nie podjęła działania określonego w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z postanowieniami niniejszego rozdziału, wszczyna się postępowanie dyscyplinarne.

2.8. Administrator prowadzi rejestr naruszeń ochrony Danych Osobowych stanowiący Załącznik nr 3 do niniejszej Polityki.

ROZDZIAŁ VIII. POSTANOWIENIA KOŃCOWE.

Niniejsza Polityka Ochrony Danych Osobowych obowiązuje od dnia 29 grudnia 2022 r. Wszelkie zmiany procedur wynikających z niniejszej Polityki wymagają zatwierdzenia przez Administratora.

SPIS ZAŁĄCZNIKÓW

Załącznik nr 1. Rejestr czynności przetwarzania.

Załącznik nr 2. Rejestr kategorii czynności przetwarzania danych (wzór).

Załącznik nr 3. Rejestr naruszeń ochrony danych Osobowych (wzór).

Załącznik nr 4. Analiza ryzyka.